UNIVERSITY OF TARTU
Faculty of Social Sciences
Johan Skytte Institute of Political Studies

UNIVERSITY COLLEGE LONDON
School of Slavonic and East European Studies

Lauren Kook

CYBER SECURITY AND RISK SOCIETY:
ESTONIAN DISCOURSE ON CYBER RISK AND SECURITY STRATEGY

MA Thesis

Supervisor: Eoin McNamara

Tartu, Estonia
21st May, 2018

I have written this Master's thesis independently. All viewpoints of other authors, literary sources and data from elsewhere used for writing this paper have been referenced.

.....

/ signature of author /

The defence will take place on at ..... */ time /*

..... */ address /* in auditorium number ..... */ number /*

Opponent ..... */ name /* (..... */ academic degree /*),

..... / *position* /

ABSTRACT

The main aim of this thesis is to call for a new analysis of cyber security which departs from the traditional security theory. I argue that the cyber domain is inherently different in nature, in that it is lacking in traditional boundaries and is reflexive in nature. Policy-makers are aware of these characteristics, and in turn this awareness changes the way that national cyber security strategy is handled and understood. These changes cannot be adequately understood through traditional understanding of security, as they often are, without missing significant details. Rather, examining these changes through the lens of Ulrich Beck's risk society theory allows us to fully understand these changes. To support my argument, I analyze statements made by Estonian policy-makers and stakeholder, demonstrating that the way that they understand the nature of the cyber domain and the drafting and handling of cyber security as a result of this understanding is best rationalized through a risk society framework.

TABLE OF CONTENTS

INTRODUCTION

The topic of this thesis will be the understanding and perception of risk and security by policy-makers in cyber security and how it translates to strategy and policy. It will focus on how the notion of security is different in the cyber domain, shifting from a more threat-centric view to a risk-centric view. It argues so through the conceptual lens of Risk Society, the sociological theory put forward by Ulrich Beck in the 1990's. The thesis will analyze cyber security through the specific case of Estonia, with particular focus on Estonian discourse of policy-makers and stakeholders.

In today's day and age, 'cyber security' is become and increasingly important and vogue topic. The topic of cyber security departs for many traditional discussions on security, along with the politics and policies that follow this discussion. My research aims to address exactly what changes have occurred in discourse at the policy-making level, with Estonia as a case study. Specifically I wish to address how Estonian policy makers understand and conceptualize cyber risk and how this influences their decisions. The concepts of risk and security have become increasingly intertwined and prevalent in the past two decades as risk comes forward as a main theme. There are many conceptualizations of the emerging risk-security nexus, but amongst the most influential is Ulrich Beck's concept of risk society. This change calls for an new analysis of the understanding of risk by policy-makers. My analysis of the conceptualization of cyber risk by policy makers will be through the lens of risk society.

This research hopes to fill a gap in the field of international relations in relation to the concept of risk society connected to cyber security. The understanding and treatment of security in the cyber domain is significantly different to that in traditional domains. This difference has not been adequately explored, and cannot be through analyzing the cyber domain and cyber security strategy through our normal conventional understanding without missing significant and key points. These difference can be understood through a lens of risk society, and we can understand the nature of the cyber domain, and the conceptualization of risk and security by policy-makers and how it effects strategy. Ulrich Beck's risk society theory has be influential and has been used in understanding modern warfare, the "transformation of war" debate, and policy decisions and

policy making. However, the concept has yet to be applied to the cyber domain in a comprehensive way. This thesis will explore the nature of the cyber domain through risk society theory, and explain the departure in treatment and understanding of security in the cyber domain.

My main research question is how Estonian policy-makers and stakeholder understand and conceptualize risk in relation to cyber security, and what effect this has on the Estonian National Cyber Security Strategy. This research question had two sub-queries. The first asks how the cyber domain is different to other domains in regards to security. The second is what is the process that policy-makers go through in order to address these differences, and what are the results in the strategies themselves. I aim to understand the thought process behind cyber security strategy and policies of Estonia, and identify how the notion of security within the cyber sector is different to other sectors, and how security had changed in recent years.

In this thesis I argue that the understand and treatment of security in the cyber domain has changed from what we have traditional seen in terms of national security. This department from traditional understanding of security translates into different handling of cyber security strategy. The cyber domain in which cyber security strategy seeks to secure is fundamentally different to other domains, and there is a keen grasp on this difference by policy-makers and by society as a whole. This change in understanding cannot be adequately understood by analyzing it through traditional notions of security. This change calls for a new lens of understanding. Ulrich Beck's theory on Risk Society and New Modernity can help us understand how the understanding of security has changed in regards to the cyber domain, including multi-sector involvement and cultural understanding and perception of risk. I present Estonia as a case study, particularly discussing and analyzing Estonian policy-makers and stakeholders discourse on risk and security in regards to the cyber domain in order to demonstrate that these changes to cyber security are best understood through a lens of risk society.

I have chosen Estonia as a case study due to the fact that it has one of, if not the most, mature cyber security strategies and cultures. This is due to several reasons. Firstly, Estonia began to develop its cyber capabilities and e-governance methods early on, allowing the government to get a head start as well as foster knowledge and esteem regarding the cyber domain. Secondly,

the 2007 cyber attacks on Estonian cyber space prompted a frenzy into action regarding cyber security, pushing Estonia into the spotlight and forcing the state to bulk up on its cyber security. Thirdly, due to both of these reasons, Estonia has established itself as an formidable expert on e-governance, e-solutions, and cyber security, which in turn has brought expert and research capability back to Estonia.

An emphasis on cyber capabilities and e-governance was establish early on in the priorities of the Estonian government, following re-independence. One stated reason for this emphasis was for cost-saving measures. Digital services save money in a number of ways, including personnel and decreased need of physical location. It has been reported that 2% of the GDP has been saved by going digital[1]. Early implementation of digital solutions had not only given Estonia a head start, but potentially also saved it from growing privacy debates[2]. As the rest of Europe and the world are soon to follow, they will no doubt face challenges regarding data sharing. However, Estonia has skipped this step, and e-ID and cross-sector leveling have already been implemented.

The 2007 cyber attacks on Estonia brought world-wide attention to the potential risks of going digital, and spurred a reaction to bolster cyber security. In Estonia, this increased the awareness of the both the weaknesses in cyber security and risks that followed digitalization. The attacked prompted Estonia to continue to expand and improve cyber security, both from a strategic and logistical point of view. However, the 2007 attacks had another consequence, which was that it brought Estonia to the forefront of the international cyber security scene. Other countries became aware of Estonia's digitalization, and they also became aware of the risks. The increased attention to Estonia, particular the reaction of the government, granted Estonia world wide attention.

As a result, Estonia not only had the advanced e-solutions and the developed cyber security strategy that culminates in a mature cyber security culture, but it has the international recognition as such. Estonia has establish itself as an expert on e-government and cyber security, which in

[1] Statistic available at https://e-estonia.com/wp-content/uploads/updated-facts-estonia.pdf

[2] There are a number of factors to consider when discussing why Estonia developed digitally, which are beyond the

[2] There are a number of factors to consider when discussing why Estonia developed digitally, which are beyond the scope of this paper. For more information see Areng, Liina "Liliputian States in Digital Affairs and Cyber Security"

turn has attracted experts to Estonia. Estonia plays host to several security organizations, most notably the NATO Cooperative Cyber Defense Center of Excellence (CCD COE). Significant documents such as the Tallinn Manual with suggestions, commentary, on international cyber security have been produced by experts in Estonia. All of this mean that Estonia is the best choice for a case study on cyber security, as it is the most mature and well-developed.

Data for my empirical research will be collected through interviews, which will allow me to get an understanding on the discourse surrounding cyber security strategy and understanding of risk and security. Interviewees will come from both the public and private sectors, including government officials, researchers at academic institutions, and experts other security organizations . This will provide a well-rounded understanding of all discourse that influences cyber security strategy in Estonia.

Interviews will be semi-structured, consisting of core questions slightly tailored to the individuals expertise or role. Questions will be focused on the interviewees understanding of cyber security, particularly how it is different to other forms of security, and underlying concepts of strategy. These questions will be designed to test for understanding and awareness of risk that is present in a risk society. There will also be an emphasis on the role of other sectors in cyber security, and the nature of policies, i.e. whether they are proactive or reactive.

My research scope is limited in two ways. Firstly, it is limited to the Estonian perspective, how Estonia deals with and perceives risks. Secondly, it is limited to the cyber domain. These two limitations will focus my research. A potential difficulty I may face arises from the unavoidable nature of the cyber domain, which is global and does not have borders. Even though my research is limited to Estonia, it can only be limited to Estonian perspective given the global nature of cyber risks. This has the potential to make it difficult to distinguish between types of risks. Furthermore, a main characteristic of risk society is that is contains many unforeseen and unintended consequences, which also makes risk difficult to both quantify and predict. However, by focusing on the Estonian perspective, the keyword being perspective, this obstacle can be avoided. The theoretical characteristics of risk can be accepted, and focus is put on which risks that policy makers emphasize.

It is worth noting to limitations of Ulrich Becks' risk society, which is used as a theoretical foundation for this paper. It is a macro sociological theory which some have argued is to vague. This makes the application of risk society both easier and trickier. It is easier because it can be applied to many different areas and many different types of research, and it's macro nature allows for much interpretation. However, this presents some issues, namely that it is easier to manipulate to fit research and arguments, and may be stretched to unrelated areas. This paper addresses this issue and attempts to avoid fitting cyber security into an ill-fitting box by analyzing and describing cyber security first, then going on to discuss the application of risk society. In this way I hope to avoid oversimplification of cyber security conceptualization and address all the complexities and concepts that characterize it.

LITERATURE REVIEW

With the growing emphasis on cyber in discussion of national security and international politics, there has come much discussion of it in the field of international relations. The treatment of the cyber domain and of cyber security has ranged from more practical discussions on how to treat it in a legal sense, to theoretical discussions on different frameworks which is best to understand the treatment of cyber in the political arena. The one thing that all literature on the cyber domain and cyber security seems to agree on is the fact that both are unique and require a special treatment.

On the more practical side, legal scholars discuss emergence of the cyber domain as a major legal field in both national and international law and the difficulties that we face as we try to set up a framework. The Tallinn Manual, an immense study on the complexities of how international law applies to cyberspace, has been published by the CCD COE with a second edition soon to be published. Less specific and analytical articles have also been published by the CCD COE, which seek to clarify cyberspace as a domain or expand on discussion of cyber law (Schmitt and Vihul 2014). In "A Legal View on Outer Space and Cyberspace: Similarities and Differences", Katrin Nyman Metcalf compares the nature of cyberspace to outer space, arguing that the two domain are "both cases dealing with areas that appear borderless, which means that traditional legal principles and rules based…specific borders, cannot apply or at least will be difficult to apply" (Nyman Metcalf 2018: 1). On the other hand, Alžbeta Bajerová conducts a more practical SWOT analysis of NATO including cyberspace as a new domain of operations, with a more traditional treatment of threats but a emphasis on cooperation between both sectors and states (Bajerova 2017: 10).

More theoretical treatments of cyber security also exist in the literature with a large range of viewpoints and arguments. Liina Areng analyzes the growth of the importance of cyber security to Estonia, offering Small State Theory as an explanation of why Estonia has become a leader in cyber security internationally. In "Liliputian States in Digital Affairs and Cyber Security", she argues that Estonia's 'small state' attributes which often excludes states from being heavy lifters in the international sphere, such as its small population and relatively new government, have in

turn allowed it to become a shining example of a digital state (Areng 2014). Lene Hansen and Helen Nissenbaum offer a completely different perspective on cyber security through securitization theory (Hansen and Nissenbaum 2009). They argue that "'Cyber security' can, in short, be seen as 'computer security' plus 'securitization'". They also discuss the difficulty of identifying specific traits or focuses of cyber security, including threats and referent objects, with much emphasis placed on the "wealth of referent objects". Also using Estonia as a case study, Hansen and Nissenbaum examine the security language behind the securitizing of cyberspace in Estonia after the 2007 attacks, ultimately stating that securitization has been partially successful (ibid: 1170).

There is a huge array of studies put out by the CCD COE on cyber security. In addition to the article already mentioned and the Tallinn Manual, the Centre also has published reports on the national cyber security structures of many nations, both NATO and non-NATO, providing in an depth look at the strategies in a structured and logical manner. "Ten Rules for Cyber Security" is another article published by the Centre which underscores ten different rule nations ought to follow when thinking about cyber security strategy . These ten rules are more abstract in nature and focus on broad concepts and ideas states ought to keep in mind, such as the 'duty to care' and the 'access to information' rules (Tikk 2011). On a more practical level, the Centre also published National Cyber Security Strategy guidelines, which provide more in depth and more concrete suggestions for states when actually drafting strategy.

The literature on risk society is the opposite to that of cyberspace and security, in that it spans across different security topics and sector, but focuses on a single theoretical approach. Risk Society was initially theorized by the German sociologist Ulrich Beck in the early 1990's, and he continued to expand and explore this theory alongside Anthony Giddens. Beck and Giddens own work on Risk Society is extensive and spans nearly two decades. This theory proves incredibly influential as is crossed disciplinary borders and permeated the literature on international politics and security studies. Beck's initial work, which lays the foundation for the key concepts such as reflexive modernization, presence of the future, and the boomerang effect, spanned across many different topics, including environmental risk and terrorism. The literature on risk society is extensive.

Risk Society theory has been applied to many different specific areas of security, by both Beck and by others. In "The 'Transformation of War' Debate: Through the Looking Glass of Ulrich Beck's World Risk Society", Yee-Kuang Heng argues specifically that risk society provides a unique and superior framework with which to understand the changing nature of war. He focuses on four elements: 'reflexive modernisation, the globalisation of risk, active anticipation and risk society's minimalist ethos'. He uses the United States as a case study, analyzing statements and documents regarding attitude and decisions made by the government. Heng argues that risk society allows us to better understand both the changing nature of war and how states make decisions regarding war. Stefan Elbe briefly analyzes the HIV/AIDS epidemic through a risk society lens, putting particular emphasis on the presence of the future in HIV/AIDS discourse. He also links the concept of the 'dangers of modernization', arguing that the spread of HIV/AIDS has been made possible by the modern advances in transportation and increasingly globalized world (Elbe 2008: 10). Risk society has also been applied to the discussion on terrorism by several authors, included Beck himself (Beck 2002).

These two literatures coincide in the discussion on risk and cyberspace put forth by Ronald J. Deibart and Rafal Rohozinski. In their article "Risking Security: Policies and Paradoxes of Cyberspace Security" they illuminate the gap in the discussion on risk in relation to cyber security, stating that while the academic and politicians alike agree on the risk to cyberspace, they ignore the concept of risks through cyberspace. They differentiate the two types of risk and treat them separately (Deibart and Rohozinski 2010: 24). Deibart and Rohozinski focus on the nature of risks themselves rather than apply the risk society framework in a comprehensive way, as Heng does with war.

CHAPTER 1: CYBERSPACE AS A DOMAIN

This section seeks to describe cyberspace as a domain and lay out the characteristics which set it apart. It begins with defining and describing the key terms and concepts that are used in the discussion on 'cyber'. It then goes on to discuss the borderless nature of the cyber domain and it effects. The nature of threats and risks which are present in the cyber domain, the actors involved, including the role of the private sector, and the non-physical nature of cyberspace is discussed in this section. Next it discusses the reflexive nature of cyber opportunity, then the role of cyber deterrence. Finally, it describes the proactive nature of cyber security strategy and policy and concludes with overarching themes.

1.1 Defining Cyber

There are many definitions floating around regarding the concept of 'cyber'. Most nations employ their own definitions, understandings, and boundaries to what cyberspace is as a domain, and what 'cyber security' means to them. Some nations have much wider concepts of what cyber security pertains to, i.e. how far national cyberspace extends to and where they can draw lines. I will discuss some of the difference in these definitions and the reasons for them, followed by a more conceptual discussion on what the cyberspace is, in itself and as a domain. I will also discuss the question of 'what is cyber security' from a conceptual point of view.

Firstly, we ask 'what is cyberspace?' Society often simply answers that cyberspace is 'the internet' and gives it no more thought, but if thinking about cyber from a security point of view, and if viewing it as its own domain, this is not clear enough. Most nations do employ more complex definitions for strategy purposes, including both the non-physical aspects as well as the physical aspects to describe what 'cyberspace' is. Here the definition comes from the Tallinn Manual on International Law Applicable to Cyber Warfare. 'Cyberspace' is:

> 'The environment formed by physical and non-physical components, characterized by the use of computers and electro-magnetic spectrum, to store, modify and exchange data using computer networks'.

Thus when we refer to 'cyberspace', we are talking about a vast interconnected system that encompasses the non-physical, i.e. the internet, and the actual physical systems which create this space. Cyberspace as a domain is a slightly more complicated matter due to this dual nature. Deibart and Rohozinski state that "in strategic terms, cyberspace is accepted now as a domain equal to land, air, sea, and space" but that it cannot be treated the same because of it is entirely human-made (Deibart and Rohozinski 2010: 16). Because of its non-physical nature, which makes up the majority of the domain, it is much more difficult to draw borders in cyberspace than it is in airspace or on land. As we will see later, this has a serious impact on the way in which cyber security functions.

But what is cyber security? Again, nations employ many different definitions in strategies and documents, ranging in complexity. For example, Norway employs the simple definition as cyber security is the "protection of data and systems connected to the Internet"[3]. Estonia, on the other hand, has a more in depth definition:

> "It is an essential precondition for the securing of cyberspace that every operator of a computer, computer network or information system realizes the personal responsibility of using the data and instruments of communication at his or her disposal in a purposeful and appropriate manner. Estonia's cyber security strategy seeks primarily to reduce the inherent vulnerabilities of cyberspace in the nation as a whole." (CCD COE)

This definition is more complex and encompasses some of the key ideas of cyber security which will be important in this paper.

However, a definition put forward by national strategies are not sufficient to conceptualize what cyber security is from a security studies point of view. If we think about the very basic concept of security as 'absence of threat towards acquired values', we begin to see an potential issue with using traditional notions of what security is when pertaining to the cyber domain. We can indeed say that the acquired value being a digitalized state. We can also identify the referent object as

[3] This definition is very close to the common definition of information security: 'the preservation of the confidentiality, integrity and availability of information' (ISO/IEC. ISO/IEC 27002: code of practice for information security management 2005). However, information security and cyber security should not be treated as interchangeable. For further elaboration see Von Somns.

national cyberspace, though this is where it begins to get fuzzy due to the difficulties in drawing succinct border in relation to 'national cyberspace'. Hansen and Nissenbaum discuss the complexities of naming a distinct referent object, instead stating that there is a multitude of referent objects, including the internet, society, infrastructures, and many others (Hansen and Nissenbaum 2009: 1157).

However, this overlooks the nature of the cyber domain, namely that there are inherent risks, or systemic risks, that can not be eliminated, only managed. Cyber security is the ongoing management of risks to and from cyberspace. Nations cannot 'secure' cyberspace for a number of reasons, elaborated further on, but must practice management of a domain of "constant transformation and a high degree of complexity" (Deibart and Rohozinski 2010: 16). By understanding cyber security as the management of risks, we acknowledge the nature of the cyber domain as it exists, and, I argue, we better understand the decisions policy-maker take and the key themes behind cyber strategy.

Lastly, I define and discuss the term 'cyber society', which is a society which is dependent on the use of Information and Communications Technology (ICT). A cyber society has digitalized and incorporated ICT into its society, including government functions and everyday life such as banking, so that it cannot function without it. For a cyber society, cyber security is of utmost importance since it is reliant on cyberspace as its main domain of business of every sort. Not every state which employs ICT is a cyber society; there is a wide spectrum in terms of the degree of digitalization and reliance on ICT in modern society.

1.2 Borderless Nature of Cyberspace/domain

One of the key characteristics of the cyber domain is its lack of borders, which is expressed in several ways. The most obvious way in which cyberspace is borderless is the actually lacking of physical boundaries, at least in the traditional way we conceive of it in security. Traditional notions of security, specifically national security, are tied to territoriality. Indeed, national security depends on the integrity of a nation's borders. However, cyber security is primarily the securing of cyber space, which, while it has of course physical roots, mostly consists of the

internet and things that we do not think of as being physical. Cyberspace is a separate domain in itself from physically territory (land, sea, air), one which does not have defined national ends and beginning (Deibart and Rohozinski 2010: 16). The non-physical nature of the cyber domain take away one of the safeguards that a state has in conventional security domains such as land of air, which is strategic depth. While kinetic warfare is limited by space and physical obstacles, cyber weapons are not (ibid).

This lack of borders is because of the nature of the cyber realm in the first place. The most prominent feature of cyberspace, and of the internet, is it interconnectedness (Nyman Metcalf 2018: 1; 11). The internet connects the government, the private sector, and civilians. Most importantly, it transcends national borders (ibid 3). It is difficult to distinguish national cyber systems and infrastructure, however to draw borders in 'cyberspace' is nearly impossible. Citizens in one country can use servers in other nations, pass and receive information to individuals across borders, and (Areng 2014: 5). The sheer number of international interactions which are available to individuals in cyberspace cannot be accounted for in this paper. The point is that it is impossible to draw succinct and definite boundaries in cyberspace, and this has significant consequences for cyber security. It becomes more difficult, as I have stated, to define what cyber security entails in a national security sense (ibid 2). This is seen by the fact that many governments have different definitions and concepts of cyber security, which results in different national strategies.

Because of this, national cyber security of any nation depends on the security of other nations as well. In this way, cyber security strategy cannot have concrete and inflexible ideas about what is or isn't national cyberspace, since cyberspace is so interconnected. This aspect is highlighted in the NCSS, which states national cyber securities are intertwined, and because of this, cyber security strategies must consider the international aspects.

The lack of common understanding in terms of what cyber security is and how a national cyber security strategy should entail can cause fragmentation in a domain where mutual understanding is necessary. If one nation has the understanding that cyber security entails that they only protect ICT, and its neighbor believes that cyber security means making sure that cyber actions of all

sectors be secure, this can jeopardize the cyber security of both nations, as international cooperation is vital in cyber security. Part of this difficulty has already been seen during the attacks on Estonia in 2007, which prompted much discussion on the triggering of Article 5 and whether cyber attack qualified. Article 5 states that allies are bound to defend one another in the case of aggression. However, debates over whether or not cyber attacks count as aggression, and if so, which attacks count and which do not, continued in the aftermath and continue to this day (Schmitt and Vihul 2014: 15). The lack of physical harm, though cyber attacks can result in this, makes it difficult to say (ibid 18). In addition to the complexities that cyber attacks have presented in terms of treaties, the new focus on cyber security has sparked a multitude of discussions on cyber law, including indetermination of jurisdiction based on the borderless-ness of cyber space as a domain.

Another way in which the cyber domain can be described as being borderless is in regards to threat and risk. In the cyber domain it is both difficult to detect threats and to identify perpetrators when an attack has occurred. This is the case both in large scale attacks such breaches in governmental systems, or in smaller instances such as cyber crime. In the case of large scale attacks, it has been proven that it is very difficult to distinguish whom the aggressor is, and even more difficult to prove it, as it had been in the case of the 2007 attack on Estonia (O'Connell 2012: 152). Even if a state sanctions cyber attacks on another state, they may do so through either individuals or organized groups which have no association with the government , 'hacktivists', and who might not even reside in either country, thus the physical location of an aggressor does not matter in some instances (Areng 2014: 5). The borderless nature of cyberspace allows cyber attacks to be conducted by anyone who has a certain skill set, which states do not have a monopoly on. In such cases, even if a state is believed to have funded or sanctioned an attack, it is very difficult to find proof. Large scale attacks need not be state sanctioned at all, however. 'Hacktivist' groups grow in number, and terrorist groups have attempted to use cyber tactics as well. These groups have the potential to cause great damage to a nation's functioning cyberspace.

Beyond large scale attacks, cyber security also entails the safety of day-to-day functions of cyberspace. In fact, cyber crime is often considered the biggest threat to cyber security, and to

the a functioning cyberspace. In theory, anyone with access to a computer, which is most of the world, has the potential to be a threat to cyber security. Cyber crime is constant and ever present, particularly in digitalized societies. But in relation to small scale attack, governments can also be involved in this, as can organized groups, and of course individuals. National cyber security, which entails the protection of the functioning of all cyberspace,

In addition to not knowing exactly from whom the threats are coming from, it is also difficult to know what the threat itself is. The pace of innovation in the information age, particularly when it comes to cyber, evolves at a pace which is difficult to track. Innovation in computer technology occurs mostly in the private sector. Furthermore, group or individuals can engineer malware which government have no idea about.

Essentially, a government does not know who will attack where, or with what. What this means is that for national security, the risk to cyberspace is omnipresent. Every system in the domain is at risk and threats come from every level. This makes it impossible to define threats to the cyber domain, and to strategize accordingly. Instead, cyber security must focus on securing or managing these risks to cyberspace, and think in terms of having a back up plan for every system to ensure the functioning of cyberspace. Cyber security ranges from securing military and government systems down to citizens securing online payment info. In a cyber society, security through management of individual citizens' cyber activities is vital, since the functioning of society is dependent on ICT and cyberspace.

I have already touched upon the involvement of individuals in national cyber security in this section, here I will expand on it. Individuals play a key role in cyber security in several ways, and can have a profound impact on the cyber domain, one being that individuals can possess the knowledge and skill sets to be a threat to national cyber security. However, individuals also play an important part in terms of what needs to be protected (Hansen and Nissenbaum 2009: 1171). When thinking of traditional national security, one which is primarily concerned with territorial integrity and physical safety of its population, the individual citizen sitting in their own home is not of direct consequence. However, this is the case with cyber security. The cyber activities of individuals need to be protected as well as infrastructures and data. This is important for all

societies, however it is essential for a cyber societies which conducts much of its business through the web.

This creates an aspect to cyber security which is not prevalent in traditional national security: that citizens play an active role in it (Harknett and Stever 2009: 12). Cyber security policies and strategies must pay attention to the role and treatment of individuals (Hansen and Nissenbaum 2009: 1171). Everyday systems and uses bare the brunt of both attacks and importance when it comes to cyber security. One of the consequences of this is that the population must be well aware of the risks, as well as have some basic level of knowledge of computer systems in order to curtail misuse and vulnerabilities. This point is made in the National Cyber Security Strategy guidelines published by the NATO CCDCOE, which outlines its suggestions and key points a nation should consider when drafting national cyber security strategies. The NCSS states that it is necessary for all levels of society to have a basic level of understanding and competence when it comes to cyber security, and strategy should accommodate this. Strategies ought to have defined plans for measuring cyber competence amongst a nations population in order to identify groups which are more at risk of cyber crime, and follow up with plans in order to fill these gaps in knowledge. In addition to this, states should consider specialized programs for educating cyber security experts and professionals.

In addition to the involvement of individuals in cyber security, there is also the involvement of the private sector. The involvement of the private sector in matters of national security is not new. Private companies have long been granted government contracts in regards to military or infrastructure projects. However, the level of involvement of the private sector in cyber security is higher, and it is also necessary. Firstly, private companies, such as banks or health providers, who utilize digital transactions must be up to date with current technology, be aware of risks, and have sufficient firewalls and protection. Transactions between individuals and private companies, private companies and other private companies, and private companies and public institutions must be secure. This requires a high level of coordination and regulation as well. This is necessary because most of cyberspace is operated by the private sector (Harknett and Stever 2009: 2). Therefore a national cyber security strategy must consider how to secure the

private sectors systems as well, and importantly, and it must also focus on cooperation with the private sector in management of risks.

Beyond the need for coordination and security in private ICT systems, the private sector is involved in the general public as well. The number of private e-solutions, e-governance, and ICT companies has grown exponentially, not only providing solutions to the private sector but also the public sector. These private companies often have the expertise that governments do not. Private companies consult on strategy and provide framework or solutions for ICT so that the intersection between public and private sector in cyberspace is difficult to separate, if at all (Harknett and Stever 2009: 10). The NCSS guidelines suggest this as well, particularly that the private sector should be involved in the decision-making process when developing strategy and solutions in order to get all relevant experience possible. In actuality, the involvement of the private sector in the way and beyond seems unavoidable when drafting strategy and when implementing it. This inclusion of the whole of society is dubbed the 'Cybersecurity Triad' by Harknett and Stever, with the three parts being the government, the private sector, and the 'cybercitizen' (11). They state that the 'triad' is necessary in order to create a resilient cyber security, elsewise important areas which are not treated in traditional security notions could be ignored (5).

As cyberspace extends into other sectors of society, cyber security also extends into other domains of security (Harknett and Stever 2009: 8; Hansen and Nissenbaum 2009: 1157). Cyber security has a direct impact on anything that is influenced or maintained by ICT, which includes but is not at all limited to infrastructure such as energy systems and military and defense systems. In all societies national security is tied to cyber security, and in a cyber society, national security is dependent on it (Harknett and Stever 2009: 3). As it is important to include the private sector in strategy, it is also important to include stakeholders from other security sectors, such as military or energy (NCSS). Cyber security includes the security of all of cyberspace, which extends to other sectors. In fact, all political and military affairs now contain some level of cyber dimension (Geers 2009: 2). This means that cyber security is also borderless in terms of sector.

Physical size and population does not have a direct effect on cyber security (some may say negative: small states may have an easier time regularizing cyber systems and securing cyberspace than a larger country with many systems and players. It is easier to innovate in a small state). Traditionally, larger and more populous states are more powerful due to having more resources, and larger territories are more difficult to conquer. Such has always been the case. However, in cyberspace the size of territory does not determine the cyber capabilities of a state, nor does the population. A small country may be weak militarily, but be more advanced in terms of cyber capabilities than its much larger neighbor, and therefore carry more weight internationally in regards to cyber issues. Furthermore, because physical distance has a deflated significance in cyberspace, states have a global reach and platform much easier (Areng 2014: 5).

The cyber domain is separated by its borderless nature. It lacks clear boundaries in many respects: boundaries in terms of threats, actors, levels, and physical borders. This makes the concept of comprehensive security a reality, cyber security is truly comprehensive security which an entire society much participate in to achieve. While other forms of security may share similarities, none can be wholly describe as borderless as cyber security it. The domain in which cyber security operates, cyberspace, is lacking in physical boundaries yet it bares many characteristics of a physical security domain. It can be treated a vital, and perhaps most important, part of national security while also having the need for new concepts of national security and new ways of approaching policy and strategy making.

1.3 Cyber Opportunity

Another things that sets the cyber domain apart from other types of domains of security, and therefore the treatment of cyber security by states, is its reflexive nature. Rather than threats being generated from outside of the border, threats are generated from a states innovation. The threats that we face in cyberspace, whether it be cybercrime, threats to national cyber infrastructure, or cyber attacks, only exist because we have created cyberspace in the first place (Von Solms and Van Niekerk 2013: 100). The level of cyber risk is dependent on how advanced a societies digital space it, the more advance it is the more they are at risk (Hansen and Nissenbaum 2009: 1155). This is especially the case when it comes to cyber societies, who

depend on ICT for the functioning of the state. These states face more risk in terms of cyber security than a state which is less developed in terms of digitalization. The cyber capabilities of others is significant as well, a individual, group, or nation is a risk only when they too possess equal or better capabilities. However, the capabilities of others is inconsequential if a state doesn't have a developed digital infrastructure. Today, every nation has some level of digitalization therefore every state is at least somewhat at risk. The unique aspect is that more advanced societies are more at risk than less advanced societies. This is the case in regards to both risks from other actors (cybercrime, cyber attacks, etc), but also basic malfunctions and failures that pose a risk.

This is not the case in regards to traditional domains of security, and national security strategies. Usually when we think of national security, what is already there dictates much of how strategy is formed. Who your neighbors are, what current political climates are like, all contribute to strategy. This goes for cyber security as well, but what exists already is less important. The cyber capabilities of a neighboring state, or a hostile group or individual, is less of threat if you do not depend on ICT that much. Also, if your digital infrastructure is not advanced or cutting edge, you may not be susceptible to new technologies problems that might effect countries whose infrastructure is. On the other hand, a nation without nuclear capabilities can still be attacked with them.

Much of the risk towards cyberspace does not stem from potential cyber attacks, but from normal system failures where there is no perpetrator or attacker (O'Connell 2012: 191). The risk is created through the digitalization itself. When a new technology is introduced, new ways in which it can fail follow suit. Computer viruses would not exist without computers. So even though advances in cyberspace and digital systems brings a wealth of societal benefits, it also brings many risks and challenges that are new for society. The risk of someone across the world gaining access to your personal information is a risk that is only possible because of the advances in the cyberspace. The internet allows us to communicate more efficiently, but it also aids in the spread of misinformation. Every innovation in cyber technology brings both positive effects as well as negative effects, which we as a society do not also know or account for. Policy makers are aware of this characteristic, and acknowledge it in strategies and in their understanding of

cyber security. The NCSS guidelines highlights this, stressing that nations should be aware of this characteristic when drafting strategy (NCSS 10).

1.4 Cyber Deterrence

Deterrence is an important topic when it come to national security. Deterrence is the concept of stopping an attack before it even begins and is often a key part of security strategy. This usually includes the building up of capabilities and pursuing one or both of the following concepts: deterrence by denial or deterrence by punishment. Deterrence by denial seeks to build up a nation's capabilities so that potential adversaries doubt that they can cause harm, while deterrence by punishment seeks to stop attackers based on fear of retribution (O'Connell 2012: 187). This concept is mostly obvious in regards to traditional and military national security, particularly in discussion and strategies regarding nuclear weapons. In relation to cyber security, deterrence by denial would consist of building up a nations cyber defense system to the point where attackers would not try. With deterrence by punishment, this might include a system of cyber offensive abilities and somehow showcasing these abilities.

However, cyber deterrence by these terms is muddled. Firstly, deterrence strategy is usually geared towards military attacks, where the actors are mostly states and the attacks are physical. Deterrence in these circumstances includes building up militaries and defensive systems, and vocalizing one's willingness and ability to retaliate. Cyber attacks may have physical consequences, but for the most part it is systems and digital infrastructure in cyberspace that is at jeopardy. Additionally, as stated before, potential cyber attacks are brought on by actors other than the state very often. An individual or a group is less likely to be put off by a governments heavy duty firewall system than a state. Also, because it is very difficult to track perpetrators of cyber attacks, deterrence by punishment is more difficult as well. If any actor, state, group, or individual, understand that there is a small chance that a state will be able to prove that they are responsible, then they will not fear retribution and deterrence by punishment will be unsuccessful.

Finally, deterrence strategy is all about deterring potential attackers. However, the biggest risk to cyberspace is not outside aggressors, but system failures that occur at the fault of no one. Unlike traditional security domains, risk is manufactured by the state itself, and the threats that the cyber domain faces does not actually have an actor to deter. In this case deterrence strategy is completely useless. This means that while deterrence may be a part of a cyber security strategy, it won't be of vital importance, since cyber attacks are not the only focus of cyber security. This in itself calls for a rethinking of national security strategy in relation to the cyber domain. States cannot simply apply similar strategy frameworks to the cyber domain and adapt deterrence strategy. Doing so would result in an anemic strategy which would poorly prepare a country in terms of cyber security, and would not encompass the nature of cyberspace (Barajevá 2017: 15).

That being said, deterrence is still at play in cyber security, but in a different way. The establishment of the NATO CCDCOE in 2004, which was founded on the idea of cooperative defense between NATO countries can be viewed as a method of deterrence. The centre focuses on training, research, and developing in order to bolster the cyber defense methods of allies. (In the CCDCOE's NCSS guidelines, there is very little mentioned about deterrence in strategy). Cyber security is a relatively new phenomenon, which means that experts and academic are trying to fully understand how it works and how to achieve it (Goodman 2010: 106). Cyber defense is still an important aspect of cyber security, which includes setting up barriers against potential attackers, but it is an ongoing learning process for policy makers.

1.5 Proactive Versus Reactive Policies

The features of the cyber domain change the way that nations must consider cyber security strategy and policy. Often national security strategies are grounded in past experiences and potential threats that are perceived by the nation. In this way strategy and policy are reactive in nature, as policy makers are reacting to past events and basing future actions on experience and history. However, cyber security strategy is not reactive, but proactive. Strategies and policies seek to lay out a spectrum of preventative measures in order to deal with a myriad of potential attacks and failures in cyberspace (Geers 2009: 7; Tikk 2011: 2). They choose to focus on things that might happen rather than things that have happened. One reason for this is because

cyberspace is a relatively new domain of interest in terms of national security, so there is a lot of history to shape strategy and policy.

This is not to say that all actions taken in the name of cyber security are proactive in nature. The famous cyber attacks that occurred in Estonia in 2007 prompted many nations to consider cyber security more seriously, so technically states are reacting to past events (Czosseck et al 2011). However, cyber strategy is not based off of a single event. National cyber strategies are not singularly crafted to respond to the famous cyber attacks, but rather to be ready to deal with anything. The attack showed the world that you do not know when an attack is going to happen and must be prepared at all times.

The proactive nature of cyber security strategy is also seen in strategy and policy not geared towards attacks, but towards reflexive cyber opportunity. As illustrated above, cyber security is not solely or even mostly about securing cyberspace from attackers, but from system failures and malfunctions. There is also a lack of experience in this for most governments. There has not been a massive ICT failure upon which strategy making could react too. Even ignoring this, however, the nature of cyberspace in that with every new innovation comes new problems, it would be unwise to focus on past events to shape current strategy. Instead, cyber security strategy must focus on countering the issues and potential problems that come with new innovation, and how to handle the unexpected.

The proactive stance towards policy and strategy is realized through the idea of cyber resilience. Cyber resilience stresses the importance of having a systems which can withstand attacks and malfunctions without widespread difficulties. This usually includes back up systems and alternative solutions, so that if a system goes down or something is compromised, then there is another system waiting to pick up (Geers 2009: 7; Harknett and Stever 2009: 12). The NCSS guidelines also stress the importance of cyber resilience in national cyber security strategy, stating that implementing the idea of resilience includes being aware of the risks of malfunctions and the level of dependence on ICT so that these problems can be addressed. Another way in which strategy takes a proactive stance is by practicing “good cyber hygiene”, which includes informing the population on safe internet practices. (O’Connell 2012: 206). Finally, most nations

employ a Computer Emergency Response Team (CERT) which is tasked with dealing with emergencies related to ICT and cyberspace. These teams respond incidents of all natures, both in case of cyber attacks, malfunctions, or system failures. The point of these teams is to be prepared for any sort of emergency occurring in the nations cyberspace.

Another way in which proactive nature of cyber security strategy can be seen through the idea of prevention. This includes the concept of deterrence, but also can be seen in the goal of cyber hygiene amongst the population. The concept of awareness amongst the civilian population is an important one all throughout cyber security strategy, but it has a role to play in regards to prevention (Harknett and Stever 2009: 12). Firstly, correct usage of ICT leads to more efficient usage and reduces the risk of user-based issues. Secondly, awareness of the potential risks by the population, such as awareness to keep passcodes private and to be wary of phishing, decreases the instances of cybercrime.

Proactive cyber security strategy and policy encompass the characteristics of the cyber domain. Cyberspace is a domain which is characteristic by inherent and systemic risk, which in turn forces policy-makers to draft cyber security strategy to look forward and be prepared for anything, particularly because of how much can go wrong on many different levels. This is distinct from other security domains, specifically traditional national security, which are more focused and had defined threats that are addressed. The cyber domain as a security domain in unique in that the threat is constant and unknown, the actors are often untraceable, and risk is generated from cyberspace itself. This creates a concept of cyber security which must focus on the management of these risks through resilience of their systems and awareness of the populations.

1. 6 Conclusion

The cyber domain lacks the clear boundaries and characteristics which changes the concept of cyber security, steering it away from traditional notions of security. The cyber domain is inherently borderless in nature, lacking first and foremost physical boundaries and being impossible to clear set national borders. The strategizing and implementation of security is no

longer contained at the state level in the cyber domain, but must include the whole of society, and thus it lacks borders in that respect as well. There is also a lack of defined threats to the cyber domain, and it is instead characterized by constant risk, known and unknown, borne from cyberspace itself. The innovation and advances that a society makes in cyberspace also threatens the security of that same space, creating a never ending cycle of risk. These characteristics all culminate in a proactive approach to cyber security strategy and policy, which emphasizes resilience and preparedness, rather than addressing specific threats.

CHAPTER 2: UNDERSTANDING CYBER SECURITY THROUGH RISK SOCIETY

I have argued that cyber security cannot be efficiently understood through traditional theories of security. In this section I discuss Ulrich Beck's social theory of risk society, and argue that the key concepts in this theory can equip up to best understand the nature of the cyber domain and cyber security. I start off with a brief introduction to risk society, including defining key terms and concepts within the theory, including reflexive modernity, presence of the future, and the role of the private sector. I then directly apply this to the characteristics of cyber security as described above, and argue that Beck's theory on risk society is the most appropriate theory to analyze cyber security.

2.1 Risk Society

Risk Society and Reflexive Modernity

Ulrich Beck's theory on risk society came into the spotlight in the 1990's as a sociological theory on modernization and risk. Beck theorized that society was moving into a 'new modernity', or second modernity as it has sometimes been called, which was distinct from what we understand as simply 'modernity'. New modernity was one in which society was governed by systemic risks and modern institutions, and one which is less defined by borders and boundaries (Beck, Bonss, Lau 2003: 4). A risk society is aware of these characteristics, most importantly the risks which govern it.

Many different definitions of varying complexity and significance have been put forward recently due to popularity on the concept of 'risk' and security. However, the one employed by Beck, and also by this paper, is not overly complex. Risk can be defined as "hazards and insecurities induced and introduced by modernization itself" (Beck 1992: 21). There is no need to overly theorize the concept of risk, but there is a need to differentiate from risk from threat. Whereas a risk has the potential to cause harm, a threat has both the potential and intent. While

traditional security communities focuses on specific threats, a risk society focuses on risk, i.e. what could happen, and how to manage the multitude of risks that arise in a modern society. Therefore, a risk society is one which has become aware and apprehensive about of the existence of these dangers – not just a society in which these dangers are present (Beck 2003: 21).

Humans have always been at risk, but what sets this type of risk apart is the origin of risk. Risks such as natural disasters or diseases have always loomed over humanity. However, neither of these risks have been created by society. Now, industrialization has created potentially grave environmental risks, medical advances such as antibiotics have created antibiotic-resistant strains of diseases. These risks have been manufactured by humans; they simple would not exist without human society. This is what is meant by 'systemic risks'; they are risks that are generated from the modern institutions that we as a society have created.

Another defining characteristic of this type of risk is its inherently global nature, which particularly applies to security and challenges conventional notions (beck 1992: 34). Risks manufactured in the new modern times does not have boundaries, they are global in nature. Conventional security often thinks in terms of the security dilemma, where one state's security means another's insecurity, however this concept is not present in security thought within a risk society. National security can never be completely disentangled from the security of other states. And while state's cannot think in terms of 'security for the human race', security from manufacture threats such as pollution and totally drug-resistant tuberculosis benefits all nations.

The concept that risk within a risk society is propagated by the society's modernization is called reflexive modernity. As we as a society continue to modernize and advance, we inherently create new risks that we can not predict (Beck, Lau, Bons 2003: 17). This has always been the case, as society's actions have always had consequences. The differentiating factor is that we are now aware of this fact. The difference between pre-modern times and the new modernity is this awareness. For example, industrialization has created numerous risks that we must deal with in current time. However, when initially industrializing, society was not aware of the potential risks it would create, nor that modernization itself inherently created risk. In a risk society, we are aware of the fact that industrialization cause risks: both that it harms human health and had potentially irreversible side effect to the environment and that there is a multitude of risk that

may accompany it that we cannot foresee. This awareness is what creates a risk society.

Awareness of reflexive modernity and the risk that accompanies it is operationalize in a society through its decision making process and its strategies and policies (Elbe 2008: 10). Being aware of a vast array of risks brought on by modernization, emphasis is placed on preparedness and management of those risks (Krahmann 2010: 349). Policies and strategies become less focused on specific threats and focus on potential risks. In security strategy and policy specifically, this means that strategies and policies become more proactive in nature rather than reactive. When employing traditional understanding of security, policy is more reactive in nature, responding to threats. In this case, strategy and policy is often shaped by past events. A previous invasion or hostility with a certain state can come to influence policy direction greatly. In a risk society, however, there is less focus on what has happened in the past and more focus on what could happen in the future, which creates a presence of the future which can be detected in the policies and strategies of a risk society. Risk societies are governed by the future, not the past. The emphasis become risk management and planning for future risks as opposed to addressing specific threat.

The Role of the Private Sector in a Risk Society

The role of the private sector within a risk society, particularly related to risk management, is unique and departs from the traditional role. The pervasiveness of risk management in a risk society creates a important role for private solutions companies, one which they happily fill as well as exacerbate. With an emphasis on risk management, the key is the word management. While the private sector sells solutions, they are involved in the management not solving of risks, which continued to create business for the private sector. In essence, Beck states that "risks are no longer the dark side of opportunities, they are also market opportunities" (Beck 92: 46).

More than being heavily involved in risk management, the private sector actually propagates risk society. The first way in which is does this is through reflexive modernity, just like all other modernization (Krahmann 2010: 352). The growing capitalist market creates risks, both known and unknown, which can be applied to all areas in modern society. However, this difference in

the private sector is that it is knowingly and purposefully contributing to these risks by proliferating, and perhaps exaggerating, the risks brought on by modernization. If the market thrives on risk, the more risk the better. This creates a 'culture of fear', which in turn makes more business for private companies and expands their roles within the sector (Krahmann 20120: 358; Aradau 2008: 151).

In traditional ideas of security, particularly in the military sector, there is often involvement of private companies. However, this cooperation is often contractual and formal. In a risk society, the involvement of private security companies is less formal and more incorporated. Part of this is to do with the fact that the growing market for risk solutions from private sector to public sector, so that the private sector tends to amass a substantial number of experts. A common trend is that more experienced and qualified security experts cross over to private sector after years in the public sector. As a result, the public sector seeks out the expertise of the private sector, which has varied knowledge of experts.

The demand for private solutions is encouraged by the unknown nature of risks within a risk society. While the public sector may be more than capable of identifying and planning for risks that they foresee, a second opinion is always beneficial. The more potential risks that are identified and managed, the better. This creates an opportunity for the private sector to identify risks (Krahmann 2010: 366).

2.2 Understanding the Borderless Nature of Cyber Security

I have argued at length that the borderless nature of the cyber domain it one of its defining features. This includes the lack of physical boundaries, the lack of sectoral boundaries, and lack of defined threats and risks. Such is the case within a risk society. A risk society is characterized by the blending of traditional borders, which is what occurs in cyber security (Beck 1992: 101). Cyberspace is has no true borders. While it is true that nations do draw lines and attempt to define what 'national cyberspace' is, this is on more of a surface level and cannot ever truly be achieved. Cyber security is a man-made domain which is not entirely physical, and does not obey national borders. This includes the question of where does cyber security end? Securing

cyberspace effect an entire society, from banking to military to energy. Nor does it effect these things indirectly, but rather directly. Cyber security must encompass all of these things, and the more digitalized a society is, the more interconnected it becomes. So as the need for cyberspace grows, and states develop cyber security, the boundaries become less and less defined.

Likewise, the blurring of traditional boundaries applies to the lack of specific threats and actors within cyber security, specifically in terms of actors. As discussed previously, a striking difference in the cyber domain as a security domain is that everyone has the potential to be a threat, and therefore everyone is a risk (Hansen and Nissembaum 2009: 1171). This includes both individuals inside and outside of national borders. This is a significant departure from traditional notions on threat. In the cyber domain there are no definite boundaries on who or what is a threat or not, and this has significant implications on the way cyber security strategy is both understood and the way it is handled. Analyzing the characteristics of the cyber domain and the implications they have on the way cyber security through a lens of risk society helps us to understand why strategy has become more proactive, risk-focused, and included more stakeholder in the process.

Lastly, the close collaboration between the private and public sector in regards to cyber security is something that we do not see in traditional security sector. Yes, there have always been military contracts between the private sector and the public sector, but this level of involvement is beyond that. We can not explain the role of the private sector, which is not just important but necessary, through traditional security theory. However if we look at it from a risk society point of view, we can see that this level of involvement is to be expected in a domain such as the cyber, which is characterized by the blurring of traditional borders.

Cyber security is approached in a holistic manner, in which both the public, private and civilian sectors are considered and included. I have expounded on the significance of the private sector both in cyber security, and its significance within risk society theory. The private sector is involved in the strategy and policy making process, and it considered a vital part. The private sector has huge significance in terms of the implementation of strategy and policy, since much, and in many cases most, of cyberspace is operated by private companies. Therefore the

significance of including the private sector in the process and implementation is of utmost importance. The importance of considering the civilian population cannot be understated. Every individual behind a computer is a risk, but they are also an important part of securing cyberspace and perhaps the biggest tool. Cyber awareness and cyber hygiene focus on educating the population of a country so that they may decrease the risk associated with common usage and protect themselves and others. The key element here is that individual are directly involved in maintaining (and threatening) cyber security. Every last individual must be included and considered in the process and implementation of cyber security, from strategy and policy to implementation.

2.3 Cyber Opportunity as Reflexive Modernity

Beck's definition of risk fits the characterization that is dealt with in cyber security. The 'risk' in a 'risk society' is one which is generated by the system itself, the very system that it threatens (Elbe 2008: 8; Beck 1992: 21; 2003). This is exactly the case within cyberspace. This risk that cyber security faces and must address comes from the advancement of cyber technology and would not exist without it. While it seems obvious that malware and cyber attacks would not exist without the existence of cyberspace, we must remember that this is not the case with other domains of security. A nation's territory is threatened by its neighbors' military aggressive regardless of it's own military advancements. Systemic risk is what plagues cyber security for both nations and global cyberspace. The risk of both cyber attacks and cyber malfunctions and malware are both systemic. This also correlates to the fact that cyber societies are more vulnerable than those which are less dependent on ICT, against stressing the idea that cyber opportunity is reflexive (Deibart and Rohozinski 2010: 19). Digitalization brings about many benefits and connects us globally, however there is a risk associated with each benefit, both known and unknown. In addition to the self-generated risk which characterizes cyber security, it is also often does not have a specific aggressor, but rather risk that features common malfunctions (ibid 24). Traditional security studies cannot be used to adequately understand and analyze cyber security, as it does not account for the origin of these risks and the effects they have on strategy and policy.

2.4 Private Sector in Cyber Security

The theorization of the role of the private sector in a risk society also aligns with that of cyber security. Because of the emphasis on risk management in particular, the involvement of the private sector is ongoing and never ending (Krahmann 2010: 352). In a risk society the inclusion of the private sector is much more informal and incorporated, which can be seen in cyber security. As I have discussed, the involvement of the private sector is of monumental importance. This is due to the borderless nature described above, but also because of the expertise that private companies bring to the strategy table. If the private sector is the origin of much of the cyber innovation in a society, than they are also the origin of innovation in terms of solutions and protecting cyberspace (ibid 365). In a risk society the private sector both creates and manages the systemic risk. This is what we observe in cyber security. The private sector advances cyber technology, therefore creating more risk, then becomes involved in the process of managing that risk. The private sector is involved in strategy and policy making, but also involved in consulting in technical terms and providing technical risk management.

2.5 Presence of the Future and Cyber Security Strategy

The borderless and reflexive nature of cyber security culminates in proactive strategy and policy which focuses on resilience. Another way of describing this quality is by stating there is a presence of the future in cyber security strategy and policy. In my discussion on the nature of cyber security strategy in chapter 1, I stated that rather than being reactive in nature, cyber security strategy is proactive, meaning that it is forward looking and seeks to address the unknown risks which plague cyberspace (Beck, Bonss, Lau 2008: 9). In this way, cyber security mirrors risk society and shows that that there is the presence of the future in strategies and policies, meaning that the future and what could happen, shapes and guides strategy (Harkett and Stever 2009: 2). This is in contrast to reactive policies, which are guided by past events and have a presence of the past. This is necessary in cyber security strategy due to its reflexive nature. Because of the systemic risks which are created by digitalization, it is impossible to make a

strategy which solely responds to specific threats. Instead, strategy must be ready for anything that the future might bring, and most importantly, be ready for action when things fail. This is where cyber resilience comes in; ICT must be agile and able to withstand constant attacks and malfunction of all nature, and when a system fails, there must be a back up in order to ensure society's functioning. However, this is not to say that cyber security strategy is exclusively forward look, but is rather both forward looking and conscious of past events.

This presence of the future which is seen in proactive approaches to cyber security is influenced by both the borderless nature and the reflexive opportunity observed in cyberspace. Cyber security strategy must be governed by the future, because of its reflexive nature. There is not going back in terms of digitalization, only forwards, which means that both innovation and risk will continue to grow. Cyber security must be prepared for these systemic risks which are borne out of advances in cyber technology. This is stressed in strategic documents, specific in the NCSS guidelines. Safeguarding cyberspace from the vast myriad of risks is of utmost importance. Additionally, the need for preparedness is seen in the establishment of CERTs, which is an essential part of any nations cyber security strategy.

Lastly, we arrive to perhaps one of the most important points and strongest examples for why the cyber domain and why cyber security is better understood through a lens of risk society, which is the fact that society is aware of these characteristics. Because there is a clear presence of the future in the conception of cyber security, this means that strategy and policy makers are aware of the reflexive nature of cyberspace, and aware that they must be ready for new risks and threats which emerge from it (Beck, Bonss, Lau 2008: 18). The emphasis on risk management is an example of this awareness. Policy makers are aware the risk to cyberspace cannot be eliminated because it is self-generated and never ending (Harknett and Stever 2009: 29). The risk can only be managed and planned for, but not stopped. This awareness is reflected in all society, from the private sector to the civilian population, who are included in the maintenance and upkeep of a states cyber security. This awareness is what defines a risk society and characterizes the nature of strategy and policy with the society.

2. 6 Conclusion

Ulrich Beck's theory on risk society is the most appropriate theory to explain the nature and functioning of cyber security, and the strategy and policy which emerges. The borderless nature of cyber security, including the lack of defined threat or actor, the total involvement of a society in the security process, and the reflexive nature of cyber opportunity are all characteristics which are descriptive of a risk society. The discourse which surrounds cyber security shows the awareness of these attributes, exemplifying the fact that society is aware of the risk which characterizes cyberspace. State's understanding and the nature of strategy and policy show that cyber security is best understood when observed from a lens of risk society.

CHAPTER 3: ESTONIAN CYBER SECURITY

In this chapter I will present my research findings. I begin with a discussion on the methodology of my research and my reasoning for choosing to gather data through interviews. I also provide a detailed explanation of my interviewing process, including my criteria for interviewees, interview structure, and method of analysis. I then discuss my findings at length and argue that Estonian policy-makers and stakeholders conceptualize the cyber domain differently to conventional security domains, and that this has a profound impact on the way that they understand risk and security within cyber. These understanding reflect in the handling and planning of cyber security strategy. This departure is best understood through analysis using a risk society framework.

3.1 Methodology and Analysis

This dissertation is a case study on Estonian cyber security, focusing on the understanding of Estonian cyber security policy stakeholders regarding cyber security. The basis of risk society stems from the understanding and perception of the society itself. Rather than a threat-based, reactive concept of security strategy and policy, a risk society in one which is preoccupied with the future, and is aware of the risks that are created by its continued modernization. The purpose of this research paper is to study the understanding of security and risk by Estonian policy-makers and stakeholders, and how this understanding has departed from traditional notions. I argue that the understanding and treatment of cyber security is fundamentally different, and these differences are best understood through a lens of risk society theory.

In this section I follow a similar structure that I have in chapters 1 and 2. I trace the characteristics of the cyber domain and their effects on cyber security strategy, analyzing the discourse of Estonian policy-makers through this lens. Firstly, Estonian policy-makers and stakeholders ar aware that of the reflexive nature of cyber opportunity, meaning that they are aware that as Estonian continues to digitize, this will continue to create risks, both known and

unknown. This awareness would not be as readily shown in formal documents or papers as it would in discussing cyber security with individual policy makers.

Secondly, the understanding is translated into policy and strategy. Strategy and policy is focused on concepts such as alternate solutions, cyber resilience, and general adaptability of the cyber security structure of Estonia. These policy characteristics are identifiable in cyber documents, however its is the process of understanding and its translation which must be traced.

Thirdly, an understanding of the lack of traditional borders of cyber security is apparent. This is something that is best to be discussed and understood through interviews, as it is not always possible to detect in policy and strategy. A emphasis on the importance of the involvement of the whole of society, or mention of need to keep citizens up to date and aware of the evolving technologies and risks, may not be present in cyber security strategy. Also, an emphasis on the importance of promoting e-solutions and ICT in both the European and international community may not be apparent. And the implication of the importance of promoting Estonia's own cyber structure and e-solutions, as well as Estonian companies, may be visible in strategy.

In order to support my argument that Estonian understanding of security pertaining to the cyber domain has changed, and is best understood through a lens of risk society theory, I conducted interviews. My goal was to capture to understanding of Estonian policy-makers and stakeholder regarding the nature of the cyber domain and the formation of strategy. I interviewed experts have contributed, influenced, and built the cyber security strategy and structure of Estonia. The reason I chose to collect data via interviews is due to the fact that it was the best way to get a firm grasp on the understanding behind policy and strategy. Simply examining policy and strategy would be inadequate in grasping the concept of security behind it, particularly the involvement of other sectors and of other parts of society.

My interviewees are from a wide range of Estonian institutions and sectors, including public, intergovernmental, and academic. In the public sector, interviewees are experts who have consulted, studied and drafted cyber security documents, manuals and strategies in Estonia. I had several different ways in which I found and decided upon my interviewees. The first step was to

contact individuals who held positions regarding cyber security at government ministries and research institutions and contact them via emails. This was mostly successful. The second way in which I chose interviewees was through examination of strategy and other important documents pertaining to cyber security and noting reoccurring names of experts who had done substantial drafting of strategy or research on cyber security. The final way in which I got into contact was from the recommendation of those who I had already interviewed.

Interviews are semi-structured, with 6 questions being prepared before hand on average, and lasting 30 – 45 minutes. The majority of interviews were conducting in person at the interviewees place of work, with (one) being conducted over Skype. Questions run along the lines of asking the interviewees perceptions of cyber security and it's key features, the nature of cyber policies and strategy, and the actors in cyber security. The core questions are as follows:

1) Is cyber security different to other areas of security?
    a. How does this translate to strategy and policy?
2) Are cyber security strategies and policies more focused on addressing specific threats or being prepared?
3) Who is involved in the strategy making process?
    a. How is the private sector/other government sectors involved?
4) How engaged is the general population in the maintenance of cyber security?
5) What do you think the biggest risk to Estonian cyber security is?
6) Is Estonia unique in the way that it handles cyber security?

Sub-questions are only asked if they follow a logical path. Likewise, questions are tailored to individual interviewees expertise, and whether expertise is rooted in technical, legal or policy experience.

The overall purpose of questions is to gage the understanding of cyber security of the interviewees in what is essential a binary test: do policy makers understand cyber security as being primarily concerned with the future, or the past? Data collected is analyzed using discourse analysis. If a interviewees answers focus on proactive policies that must be prepared for unprecedented risk that do not stem from perceived threats, but rather form the nature of

cyberspace itself, this signals a presence of the future which is a defining feature of a risk society. This is mostly addressed through questions 2 and 5. Carefully attention has been paid to the description of the risks and actors involved in cyber security, along with the most important features of strategy and policy.

Another goal of the questions is to get a firm grasp on the interviewees understanding of the borderless nature of cyber security, or the blurring of traditional boundaries which is seen in risk society. Questions 3 and 4 and mainly geared towards this, and question 5 to a lesser degree. I focus specifically on the involvement of other sectors, besides government, in order to detail the importance of cooperation and horizontal collaboration in regards to drafting and implementing cyber security strategy. I also placed an emphasis on the understand of risk and perceptions of threat in order to showcase the proactive nature of strategy and the presence of the future.

It is important to note the ways in which I have avoided bias and influencing the data collected in interviews. First and foremost I avoided using words which might influence or steer interviewees answers unnaturally; mostly words which I considered 'buzzwords' in my research. These are terms which have been discussed mostly in chapter one of the dissertation, and I therefore avoided my own understand of cyber security steering data. The avoided words were 'borderless', 'risk management', 'reflexive', and 'resilience'. Instead, I waited for interviewees to use these terms themselves and then asked them to elaborate. I also avoided using terms found in Beck's risk society theory, such as 'risk society' and 'presence of the future', and overall avoided any theoretical questions. These measures were taken in order to ensure the integrity of my data and get a grasp on interviewees own experiences and views.

3.2 Research Findings & Analysis

This section will present the findings of my research and analyze them. This will include a analysis of discourse concerning the nature of the cyber domain and the management of risk in Estonian cyber security strategy. This analysis will mirror my the argument I have presented in this paper already, supporting the argument that viewing the understanding and treatment of the cyber by policy-makers is best analyzed through a risk society framework. I will present direct

quotes from my interviewees and discuss these statements and how they exemplify a departure form traditional understanding of security.

Classifying Estonia as a Cyber Society

I have argued that Estonia is a ideal case study for studying cyber security due to its high level of digitalization and focus on the cyber domain. I have introduced the concept of cyber society, a society which is dependent on ICT, and presented Estonia as an example of cyber society. Estonian society is extremely dependent on digital services, relying on ICT for everything from taxes to banking to government records. This dependence is realized by cyber security experts as well; all interviewees stressed how important ICT is for Estonian society. Dr. Rain Ottis, from Tallinn Technical University, stressed this early on in his discussing of Estonian cyber security:

> *"Estonia is still very dependent [on ICT] and cyber security is still very important…Cyber security in Estonia is not a nice to have thing, it is a must have thing and therefore we should put emphasis and effort there."*

Here Dr. Ottis states that cyber security is an essential part of the functioning of Estonian society, not merely something that is 'nice to have'. This puts the importance of cyber security for Estonia into perspective. Other experts also talked about Estonian dependency on ICT:

> *"The dependency on IT grows and it grows fast."*
>
> - Taimar Peterkop, RIA

> *"We are very dependent on the e-services, and there is no going back to paper."*
>
> - Uku Särekanno, RIA

Clearly there is an awareness of the extent of dependence on ICT and the significance this puts on cyber security. The fact that Estonia is a cyber society is significant, as is the awareness of this fact by policy makers, which will be discussed later in this chapter. This further stresses my point that Estonia is a crucial case study because of its dependence on ICT. Throughout my interviews, it was extremely clear that Estonia is a cyber society and is dependent on e-services. This is supported by the nature of the Estonia ID-card system, which requires all citizens to have

the electronic card with which all government services, and the overwhelming majority of private services, reply upon. Nearly all government business is handled through e-services, and 99.6% of all banking in Estonia is done through the web (e-stonia facts). Dr. Ottis' statement reiterates the point I have made earlier in this paper: with increasing dependence on ICT comes an increasing importance of cyber security.

Borderless Nature of the Cyber Domain

I argue in chapter 1 that one of the most defining features of the cyber domain is its borderless nature. In risk society this is described as the blurring of traditional boundaries that is inherent in new modernity. This section discusses the qualification of the cyber domain as borderless by policy-makers and stakeholders in Estonian cyber security, focusing on their description of the nature and conception of what sets the cyber domain and cyber security apart.

One of the most important parts of determining how experts understand cyber security as a whole, what defines it, and how it is different. When answering this question, experts almost always started off their discussion by stating the borderless nature of the cyber domain or cyber security. Some directly compared this to the nature of conventional security, stressing that this was a quality that was extremely important and determined how policy makers handle cyber security. Pilleriin Lillemets, a researcher at the Baltic Defence College (BDC), said:

> *"One defining part of cyber security is the borderless nature of it; it makes it more complicated. You cant only have your very national policy or strategy because you are very much connect with every part of the world."*

An expert at the Ministry of Economy and Communication, which is the ministry in charge of drafting Estonia's national cyber security strategy, began discussion by saying:

> *"The thing is that cyber security doesn't have any borders; …when you talk about cyber security, it is international, cross border and effects every person. In short I think cyber is quite wide, you cannot put it in certain boundaries, its impossible."*

Mr. Siim Alatalu, of the CCDCOE, also spoke about the difference of the cyber domain compared to others, specifically stating that the fact that it was man-made set it apart. So cyber security is set apart by its borderless nature, which is something that must be considered when talking about it. For several of the interviewees, this was the first thing that was explicitly mentioned when asked to described cyber security and how it is different. From the above statements alone we can see a clear understanding of the borderless nature of the cyber domain, and we will see how it effect the nature of cyber security strategy. Not only did experts simply qualify it as borderless, but many went on to describe the specific qualities which lack boundaries that had been also described in chapters 1 and 2. The following subsections take a closer look into what specific aspects of cyber security were lacking in borders.

Lack of Defined Threat

It is impossible to make a inclusive list of all of the risks and threats to the cyber domain. Estonian policy makers are aware of this and highlight the fact that much of the risk and threat are unknown and impossible to track, and that it is futile to attempt to focus on specific threats. This is something that guides strategy and policy.

The interviewee at the Cyber Defence College elaborated on the idea of threat, focusing on the unknown features of it:

> *"I think what makes it different the unknown part of it."*

Taimar Peterkop, the head of the RIA, specifically contrasted the nature of threat in cyber security to that of traditional military security:

> *"If you look at military security, for centuries the threat has been to the east and they've used the same routes, so its always the same approach […] so you know what to do. But in cyber it changes, but every year you have a completely new threat."*

Mr. Peterkop also detailed the specific routes that had been utilized in military attacks against Estonia for centuries. This highlights a very important point: in military security for Estonia,

threats are tied to physical borders and therefore easy to understand and know, and they are often constant. The tools may change but the routes do not. But because cyberspace is constantly expanding and innovating, the tools and the routes change. This makes it very difficult to zero in on specific threats and make precise strategies on past knowledge, as it is with conventional security. When discussing the process of scenario-based strategies, Mr. Peterkop elaborated on the necessity to focus on system failures rather than try to narrow down to most likely scenarios:

> *"We are looking at scenarios based on the systems which are the core of our digital society, we are not looking at the threat vectors, because are too many of them."*

So policy makers do not focus on specific scenarios, but rather focus on making a detailed plan on how to protect critical infrastructure due to the difficulty of pinpointing such specific scenarios. There are simply too many risks to consider to be able to focus on specific types of threats. Further more, there is also an issue with understand what is an attack, as Ms. Lillimets explained:

> *"We are constantly under attack, but also what is an attack? Our networks are always attacked or penetrated or tested for vulnerabilities."*

There is acknowledgment of the continual risk to the cyber domain, and this results in the focus leaning away from specific threats or specific attacks. Instead, there is a mentality of needing to be ready for anything which is created by this uncertainty:

> *"We're not pointing finger and saying you are likely to attack us, we're saying here are the kinds of things we are worried about and here are the things we can do in order make our system more resilient to various types of problems"*
>
> – Dr. Rain Ottis, TTÜ

> *"You need to have a holistic approach because you really don't know what kind of attacker you are facing and you need to have collaboration."*
>
> – Dr. Robert Krimmer, TTÜ

> *"And it is harder to know if there is going to be an attack on your systems, but making sure everyone knows their basic cyber security isn't."*
>
> - Pilleriin Lillemets, BDC

Based off of these statements, we can observe several thing. Firstly, that the Estonian cyber domain is constantly plagued by threats which are difficult to discern. Secondly, Estonian policy-makers and stakeholders are aware of this blurriness and have reacted to it by focusing on a more comprehensive approach to cyber security. This lack of focus on specific threats is something that is not seen often, particularly when dealing with security. However, if you view this from a risk society point of view, this is understandable and we can see that policy-makers must view cyber risks in this manner given the nature of the domain.

Lack of Defined Actors

A contributing factor to the lack of defined threat is the lack of defined actors. There are two levels to this: lack of defined risk actors and lack of defined security providers. This is another feature of the borderless nature of the cyber domain detailed in chapter 1 and 2. The cyber domain lacks the traditional boundaries in terms of sector that conventional security domains do. This has significant consequences on cyber security, mainly that a more comprehensive approach must be taken. The lack of defined actors operating in cyber security means that everyone is both a risk and a security provider.

Everyone is a Risk

In cyber security everyone who uses a connected device is a potential threat to security and therefore a risk. If Estonia is a cyber society, which is supported by policy makers statements, then everyone in a society is digitally connected and therefore everyone is a risk. We can add this to the already long list of risk actors explained in previous chapter: states, foreign individuals, and groups of individuals such as terrorist groups of 'hacktavist' groups. The head of the Cyber Security branch at RIA had this to say about risk actors in cyber:

> *"This is a big difference between cyber security and physical security: each and every user is a possible risk, each and every entity can effect cyber security in general."*
>
> - Uku Särekanno, RIA

On a similar note, Ms. Lillemets stated:

> "*The biggest problem is people, the human error and the person sitting behind the desk is the biggest cyber risk."*

The main reason that everyone behind a desk is a risk is due to both the simple risk of an individual not knowing how to properly protect themselves in cyberspace. While not everyone will be careless, there has to be an understanding of the potential of risk.

Beyond this acknowledgment of basic human error as a potential risk, interviewees also touched upon the point that individuals have a heightened ability to act as threat actor as a 'lone hacker', or an individual acting alone in their cybercrime. There are also groups of individuals, which interviewees often referred to as 'hacktavists', both in a non-state capacity and in a state-sanctioned capacity. Finally, there are state actors in this matrix. This was the most common classification of potential threat actors, though there was discussion of how these three 'levels' interact and mesh. The overarching theme was that there we a great deal of potential threat actors to Estonian national cyber security, so much so that it was not fruitful to try and identify them and strategize specific responses to them.

Security Providers

Cyber security is also different from traditional security in terms of where security comes from and who provides security. This is another facet of the lack of boundaries in cyber security. In conventional security the state is the provider of security and the main actor within security. However, due to the nature of the cyber domain this approach is not feasible, and viewing the state as the main provider of security ignores the importance of the involvement and agency of other actors in security. This is clearly the case with regard to Estonian national cyber security, and was evident through interviews. The securing of Estonian cyberspace is achieved through the public sector, the private sector and through civilians. Interviewees focused on the importance of a bottom-up approach to cyber security, stressing the role of the private sector and the general public. Piret Pernik, a researcher at the ICDS, elaborated on this:

> *"Because of the fact that everyone owns a device [there is a] personal responsibility that everyone has to take care of there own personal cyber security. This isn't the case in traditional military security where the state provides security; in this sense the responsibility is spread."*

This shows that individuals in a society are responsible for cyber security as well, not just the government. Mr. Peterkop also stressed the importance of a holistic approach when considering how to secure national cyberspace:

> *"I think the main different between cyber security and conventional national security so far is that approach to cyber security has to be distributed, its not a top down approach like you have in military security."*

One of the ways that citizen are involved in the securing of cyberspace is through participation in the Cyber Unit of the Estonian Defense League, a voluntary organization which helps monitor cyberspace:

> *"People are involved through the Cyber Defense League[4], there's a network of IT administrators who monitor the internet and give feedback, and that happens also on local level…there is a lot of communication there."*
>
> – Dr. Robert Krimmer

The Cyber Unit was mentioned often by interviewees. The emphasis on this voluntary force, sometimes referred to a 'cyber militia', and its existence in the first place, shows the level to which cyber security practices in Estonia are spread out and shared by society. The concept of a 'militia' is not something that has been considered integral or even useful in recent times, yet the Estonian model for the Cyber Unit is been studied and considered as a model for other nations as well. This shows that the involvement of civilians in cyber security is indeed different to that of traditional security.

This is also extended towards the private sector, which plays a significant role in the maintenance of cyber security. A large majority of critical infrastructure, such as banking, is

[4] The 'Cyber Defense League' is the former name of the Cyber Unit of the Estonian Defense League, interviewees sometimes referred to it as the 'CDL'.

actually maintained and developed by the private sector, a fact that interviewees stressed as an important part of the necessity to consider all parts of society as upholders of security. This means that the private sector is also a integral part of securing cyberspace and has a huge amount of responsibility in terms of cyber security and the functioning of Estonian e-society. Mr. Särekanno stressed this need:

> *"A number of risks are associated with the essential service providers in the private sector and its up to them to make sure they have the capabilities and ability to handle them. So it requires a lot of cooperation and mutual effort to build up a solid baseline security."*

Mr. Särekanno touches upon an important point: that the need for multi-sector approach in cyber security in turn creates a need for cooperation and communication. The strategy address this and drafts policies which regulate the security measures taken by the private sector:

> *"There is a good cooperation because they [the private sector] need to follow security standards. Also in law, the private sector has to implement those security measures."*
>
> - Piret Pernik, ICDS

The private sector's role in the securing of Estonian cyberspace is an essential part of cyber security, and the strategy and policy reflect this in their treatment of it. Strategy and policy not only regulate the security practices of the private sector, but also place an emphasis on partnership and working together:

> *"We put a lot of emphasis in building this community and a public-private partnership"*
>
> - Taimar Peterkop, RIA

> *"It is extremely important that the agency [RIA] is viewed not only as a supervisor but as a partner in cyber security."*
>
> - Uku Särekanno, RIA

> *"[There must be] cooperation between government, private sector, and academy in order to integrate cyber into lives of everyday citizens…cyber security should be a part of our every day lives, I think this is the biggest change in Estonian society*."
>
> - Madis Raaper, MEAC

Furthermore, Mr. Peterkop also discussed the involvement of the private sector in terms of filling in the gaps where the government is lacking:

> *"The government usually isn't very good at procuring e-solutions. The private sector delivered more than expected. Last autumn we had ID-card crisis, we need a specific competency which we lacked, we turned to a specific company and they gave us the technology we needed."*
>
> – Mr. Taimar Peterkop, RIA

Other interviewees also discussed this, stating that the majority of innovation comes from the private sector, and there is a high level of cooperation between state and private sectors in order to maintain a functional system. Beyond this, every interviewee talked at length about the involvement of the private sector and 'relevant stakeholders' and experts from various institutions in the strategy drafting process itself:

> *"So currently we have four or five different workshops with different stakeholders, and I would say that most of the key players form the community have been engaged."*
>
> – Uku Särekanno, RIA

> *"We invite all research institutions, academies, universities, private sector, ministries, so in this sense I don't think this is very common for normal procedures."*
>
> - Piret Perdik, ICDS

> *"Everybody is [involved]. We include all relevant stakeholders from public and private sector, academia and non-profit as well."*
>
> – Raul Rikk, EGA

One of the strongest themes from the interviews was the stress on the involvement of all stakeholders in the policy-making process, and the important of considering everyone in terms of practicing security. Thus we cannot explicitly label actors in Estonian cyber security regarding who practices security, or who provides security. These sentiments expressed by interviewees were also seen expressed in the second national cyber security strategy of Estonia. Principle 4 states that:

> *"Cyber security is ensured in a coordinated manner through cooperation between the public-, private- and third sectors, taking into account the interconnectedness and interdependence of existing infrastructure and services in cyberspace*."

– Estonian National Cyber Security Strategy, Principle 4

The entire society is responsible for the maintenance and security of cyberspace, and this is an attitude that held by Estonian policy-makers and stakeholders.

Bug Bounties and Penetration Testing

A specific example of the significance of cooperation that interviewees spoke about was the importance of penetration testing. This is along similar lines to the cyber hygiene test in development. Instead, this service is offered by the Estonian government, RIA in particular, to private companies in order to test the resilience and strength of their firewalls:

> "*We have contracts where we do penetration testing and we do it with government funding. And the companies get very useful information regarding weaknesses in the system, but for the government the benefit is that they essentially are doing the necessary adjustments that are needed."*
>
> – Uku Särekanno, RIA

Another example of this is the reserve: bug bounties. Dr. Rain Ottis described these bug bounties and why they are unique and important:

> *"Most cyber incidents happen because of errors in programming, so companies offer rewards for anyone who can find a bug and report it… This is different from a more state-centric view, where the state has full power and everyone must work for you."*

As Dr. Ottis stressed, this concept is a very different take on conventional view of security, where the state take full responsibility. Both the public and private sector take advantage of the borderless nature of the cyber domain, specifically the fact that every individual takes an active part in it. This is another way that Estonian strategy manages risk within the cyber domain.

Cyber Opportunity in Estonia

With increased dependence on digital services and ICT, Estonia's need for strong cyber security increases as well. This is one of the defining traits of the cyber domain and of a risk society. I have argued that as cyber security is best understood through a lens of risk society theory, increased digitalization brings more risk to the cyberspace of Estonia. As Estonia is a cyber society that keeps digitalizing and relying on these services, it is also exposing itself to more risk. While it is enormously beneficial for Estonia to continue this process, it also creates risk and makes the country vulnerable. It makes it vulnerable to attacks, but also to the systemic risks which characterize and define a risk society. These systemic risks are borne out of digitalization and created by the system, i.e. cyberspace, itself. These risks are malfunctions and malware which come from the programming or failure of systems, and are not enacted by individual, groups, or states. In a risk society, people are aware of these systemic risks and the reflexive nature of modernization.

Estonian cyber security policy makers and stakeholders are aware the systemic risk which characterize their cyber society, and the reflexive nature. Interviewees often specifically addressed the reflexive nature of digitalization:

> *"We are very dependent on these things, and vulnerabilities is a nature part the bigger the system is the more vulnerabilities there are. When we are completely reliant on these service it can backfire at some point."*
>
> - Pilleriin Lillemets, BDC

> *"Because we are so dependent on cyberspace so we are more vulnerable than other countries."*
>
> - Piret Pernik, ICDS

> *"Firstly, we are very dependent on the e-governmental services, which makes us very vulnerable and we have to pay much more attention to cyber security than other countries."*
>
> - Uku Särekanno, RIA

> *"Now that there is a higher level of e-voting, that makes us more attractive to state level attack, and we need to monitor, and RIA is doing a lot"*
>
> – Dr. Robert Krimmer, TTÜ

This shows that cyber security experts are indeed aware of the reflexive opportunity that comes along with advancement of ICT. Interviewees stated that cyber security was more important in Estonia because it was advanced and reliant on these systems. Estonia's modernization and innovation of ICT, e-services, and e-governance also exposed it to risk it was no before. The interviewees were aware of this face and the necessary marriage between modernization in cyberspace and vulnerability in cyberspace.

There was also a significant amount of discussion concerning the reflexive risks which stem from the system itself. The risks themselves are lacking the traditional 'from whom' actors, and instead are systemic. Interviewees discussed these risks at lengths, stating that these systemic risks are the most common:

> "*Most cyber incidents happen because of errors in programming.*"
>
> - Dr. Rain Ottis, TTÜ

> *"If you look at stats about the incidents are reported to CERT, most are related to malware."*
>
> - Uku Särekanno, RIA

Most of the risk to Estonian cyberspace is not cybercrime or cyber attacks, as some might expect, but everyday malfunctions, or systemic risks. And Estonian policy-makers pay keen attention to this, and are aware of this fact. In addition to awareness of the nature of these risks as systemic, there is also a acknowledgement that these risks are the biggest threat to cyber security.

> *"I think that the more the discussion goes on the more it becomes about the everyday than the big catastrophic incident."*
>
> - Pilleriin Lillemets, CDC

This statements shows that experts consider everyday cyber security, such as systemic risks, as the biggest threat to cyber security in Estonia. This was a common theme discussed by interviewees. While they acknowledged the importance of planning both for cyber attacks, small

and large, and everyday systemic risks, there is an agreement that these systemic risks ought to be the focus because they are the most common. This sets cyber security apart from conventional security because large scale attacks are not considered the main risk to be dealt with. This understanding has developed as cyber security is discussed more and more, because society become increasingly aware of these systemic risks and adapts accordingly.

> *"It ended up in a way that the strategy focuses on the capabilities we need to develop in order to cope with the modern world."*
>
> – Uku Särekanno, RIA

The Nature of Estonian Cyber Security Strategy and Policy

All of these characteristics of the cyber domain and the concept of risk culminate in a proactive approach to cyber security strategy and policy. Through Beck's risk society lens, we can rephrase this by stating that policies possess a presence of the future. Strategy and policy cannot be reactive in nature, especially as the culture of cyber security evolves, because of the borderless nature of threats and actors. It must focus on preventative measures due to the unknown factors that plagues the reflexive nature of the cyber domain. This is why there is a significant presence of the future in strategy and policy, and why they focus on resilience and agility. Estonian policy-makers do understand the cyber domain in a specific manner which can be understood through risk society, particularly because they are aware of the reflexive nature of it. Because of this, Estonian cyber security strategy expresses this understanding through proactive policies with a significant presence of the future. Taimar Peterkop characterized Estonian cyber security strategy as such:

> *"You have to be very agile and flexible and proactive in cyber security… We cannot prepare for every scenario, in conventional, you have specific scenarios, in cyber you have to be much more abstract."*

The notion that strategy and policy must look towards the future was very clear from the interviews. This is mostly shown the focus on the concept of resilience, which came off as extremely important. All interviewees stressed the concept of resilience, and agility, as the most important part of cyber security:

> *"The cyber strategy is about resilience. It has different components, but we are mostly concerned with building resilience"*
>
> - Taimar Peterkop, RIA

> *"It is more about cyber resilience, specific threats are considered as well but the strategy is more based on building capabilities."*
>
> - Uku Särekanno, RIA

> *"We're saying here are the kinds of things we are worried about and here are the things we can do in order make our system more resilient to various types of problems."*
>
> - Dr. Rain Ottis, TTÜ

These three statements exemplify the rationale behind resilience in cyber security. It is difficult, if not impossible, to make a cyber security strategy or policy which focused on specific threats. Discussion of resilience often went hand in hand with discussion about the nature of risk to cyber security. This shows that that policy makers are more concerned with planning and risk management than having a strategy that is specified towards threats. This shows that policy-makers are aware of the nature of the risk they are dealing with as uncertain, reflexive, and never ending. There is a big emphasis placed on the idea of alternate solutions as well in regards to cyber resilience. Dr. Robert Krimmer described the resilience of the Estonian e-voting system:

> *"The whole election system is designed so that if the system is malfunctioning, you can still cast a vote because its an advanced voting system"*
>
> – Dr. Robert Krimmer

Interviewees stated that this is the way the Estonian infrastructure and e-services have been designed, so that if there is a failure, there will not be a failure of access to services or information. Building alternative solutions into the system builds a resilient system that ensures the functioning of the e-state even when something goes wrong, which Estonian policy-makers

and stakeholder always assume will. Subgoal 1.1 of the Estonian cyber security strategy centers around the importance of building alternative solutions.

Additionally, there was more emphasis on the importance of the role of cooperation in cyber resilience, against stressing the borderless-ness of the cyber domain and how it translates to strategy and policy:

> *"Is mostly about government, how to achieve resilience though education, cooperation between different sectors, through academy, through raising competence and I think also we need functioning e-state."*
>
> - Madis Raaper, Ministry of Economic Affairs and Communications (MEAC)

> *"Everyone understands that there is no such thing as 100% secure device, so sooner or later you will be hacked, so its how quickly can operate normal [functions]. You can see this thinking in previous strategy, it was about designing resilience."*
>
> - Piret Pernik, ICDS

Therefore building a resilient Estonian cyberspace must also consider all the relevant stakeholders. As the cyber domain spreads across all sectors of society, there must also be a focus on making sure that the concept of resilience is present across all of the cyber domain. The importance of involving 'all relevant stakeholders' was a reoccurring theme that stuck out in all interviews. This is something that is different from conventional understanding on security; we would not see the same thing happening in the drafting of the Estonian National Security Strategy.

The specific concept of risk management was also a key theme along with resilience and preparedness. The emphasis on the risk management as being the center for cyber security highlights the fact that cyber security is an ongoing process:

> *"The basic concern for us is preparedness and risk management. That's the basic concern. We really want the private and also public sector to assess their risks and do the proper adjustments in line with assessments."*
>
> – Uku Sarekanno, RIA

> *"[This is] why alternative are important and the system needs to be resilient enough to withstand attacks if they might have. This is what we are aiming for, not to say no to technology but to manage the risks."*
>
> – Taimar Peterkop, RIA

This statement in particular specifically indicates the awareness of the risks that come from modernization. Policy-makers and stakeholders are aware that innovation breeds more risk, but rather than curtail modernization of the cyber, they chose to move forward in a way which manages these risks that are produced. This is what cyber security is to Estonia, the management of the risks which are produced by the cyber domain. The idea of managing also implies the continuity of risk in the cyber domain. Cyber security must be the management of risks because there will always be risks:

> *"It is something that has been planned for and you engage the relevant parties from private and public sector, and you through it and survive because there is no way, absolutely no way, of building a 100% secure system. If you have to plan for partial failure and this is normal."*
>
> – Dr. Rain Ottis, TTÜ

> *"When it comes to do with what to do in order to protect their computers, and personal data, they might understand the threat, but there is a continuous need to improve the skill on what to do exactly."*
>
> – Mr. Raul Rikk, EGA

Estonian cyber security strategy is much more focused on building a resilient and agile system over all then focusing on specific threats. This is because of the nature of the cyber domain as one which is borderless and reflexive. Estonian policy-makers understand that strategy must focus on managing the risks due to the reflexive nature of these risks, i.e. system risks, and the fact that continued innovation will also continue to produce more risks. Estonia has taken the stance that cyber strategy must be prepared for the unknown risks and threats they will face in the future, rather than one which safeguards against the threats they have faced in the past.

ID-Card Crisis

One example of the nature of the Estonian system which displays these attributes is the ID-card crisis of 2017. The National ID-card of Estonia, which is mandatory for all citizens, is the foundation of the e-service system. Voting, banking, and government services revolve around the ID-card, which is based off a electronic chip. In 2017, the security of the system was called into question when a vulnerability was found it the software, potentially exposing citizens to identity theft. This was a topic which came up frequently in interviews, and, surprisingly, was treated as a positive thing:

> *"We needed an id crisis like this, because it showed that our government is able to react quickly and effectively. It also automatically enhances the level of trust in e-society and in government. Trust in governments fluctuates, trust is e society doesn't fade away."*
>
> – Madis Raaper, MEAC

This positive spin on the crisis is founded in the idea that this vulnerability was brought to the attention of the government before it was a major issue. And indeed, it was fixed before any citizen's information was exposed or stolen. This was also expressed by Mr. Alatalu of the CCDCOE:

> *"It was a good thing to be exposed to it before any damage was done."*

Likewise, Dr. Ottis spoke about the incident as being a successful demonstration of the agility of the Estonian system, and the important of alternative solutions in a situation such as this:

> *"Last year we had a problem with the ID card, one way to solve this would have been to say: 'ok we have problems with the ID-card so we'll temporarily move to Mobiil-ID.'"*

The attitude that experts took towards the crisis shows the underlying attitude towards cyber security as a whole in Estonia. It is better to be prepared for anything, so that the system will be able to adapt quickly in order to fix an unexpected issue. This was the case with the ID-card crisis. A system which expects failure is able to handle it better than a system which does not. The ID-card crisis is an important example for another reason, in that the solution was presented

to the Estonian government by a private company. Interviewees explained that an IT company approached the RIA on its own in order to suggest a possible solution to the vulnerability. This shows the importance of the cooperation between the public and private sector when it comes to cyber security.

Role of Education and Cyber Awareness

There are many methods of building up cyber resilience, however one method which sticks out as both very important and indicative of the borderless nature of cyber security: the role of education and cyber awareness. The stress that is put on the importance of cyber awareness of the entire society reiterates the fact that cyber security must involved all sectors. I have already discussed the importance that cyber experts placed on the role of individuals in securing cyberspace, now I discuss the way it is dealt with in strategy and policy.

One of the key terms here is cyber hygiene, which refers to basic digital security for the individual. Dr. Rain Ottis describes it as such:

> *"Cyber hygiene is cyber equivalent of brushing your teeth; it should be possible for everyone. Anyone who is able to pick up an iPad, and do something there should also be able to get a bit more aware of cyber threats and basic security best practice."*
>
> - Dr. Rain Ottis, TTÜ

So here we see that there is a clear idea that anyone and everyone should be able to practice basic cyber security practices, and that this is something that can be expected in a cyber society such as Estonia. To implement this, policy makers stress the importance of starting at the base of society again, and focusing on a bottom-up approach:

> *"I think we should start from grassroots level, and we should go to school system. I think step one is, and I am not saying this will be included in new strategy but it will pan out eventually, I think there will be certain cyber hygiene course for elementary school kids"*
>
> - Madis Raaper, MEAC

> "*With the campaigns and cyber hygiene testing and basic teachings in school that's the way we try to handle it.*"
>
> - Uku Särekanno, RIA

So there is a importance placed on implementing these awareness measures at the starting point of society, schools. This is built off of the recognition that individuals pose a risk to cyber security discussed earlier. As individuals are both risks and also directly involved and connected to the cyber domain, they must be considered in strategy. Interviewees stated that schools was a focus of this, and that this focus would continue to grow in the future strategies. However this extends outside of schools as well:

> *"I think that the…we could increase our own cyber security and decrease the vulnerabilities when we educate everyone from my grandma to my prime minister…because it is sometimes the easier things you can do for your own cyber hygiene that can prevent bigger things from happening."*
>
> - Pilleriin Lillements, BDC

In regards to the military education course at the Baltic Defence College, Pilleriin Lillemets discussed the process of training all student in very basic cyber security practices, and also the role of the cyber hygiene test:

> *"All the students who come in have to take the cyber hygiene test, and this is where it starts."*

Similarly, Mr. Särekanno discussed the development of program designed to help individuals assess their security practices:

> *"Speaking about cyber hygiene, we are putting more and more effort into this. We are currently testing and piloting a system which people can test their own cyber security skills and assess your cyber habits."*
>
> – Uku Särekanno, RIA

Again this shows the importance of every individual in Estonian society to be at the very least educated and informed on basic cyber security. The emphasis on cyber hygiene and education is one way in which Estonian cyber security strategy manages risk. There was an understanding amongst interviewees that cyber hygiene and basic awareness of the population concerning cyber

security practice could prevent future incidents from happening and disrupting the functioning of Estonian cyber society. Once again, we can see that this was translated into the second strategy. Principle 5 states that "cyber security starts with individual responsibility for safe use of ICT tools". The role of raising awareness is a constant theme through the strategy, and is specifically addressed in several of the subgoals (Estonian NCSS). In this way we can see that Estonian policy-makers and stakeholders focus on managing the risks posed to the cyber domain by the involvement of individuals, and explicitly stated that this could prevent future incidents.

The Attribution Issue

The act of attributing attacks is another issue that was discussed by interviewees. There were several component to this issue. One issue was simply that it was difficult to attribute attacks, given the nature of the cyber domain. It was stressed that not only was it difficult, but that Estonia rarely had the resources to spare in what it a lengthy and expensive process. This was especially due to lack of manpower. Dr. Rain Ottis stressed this heavily:

> *"But in most cases today if you have a serious opponent you are going to have trouble identifying you are under attack, let alone attributing."*

> *"Coming back to strategy, especially smaller countries like Estonia, to some degree strategy must be agnostic in terms of who is attacking us. We very rarely have resources to attribute attack. Even if we do attribute to state actor, realistic what can we do? We can only talk about it in international forums."*

This particularly was stressed by technical and defense experts, who discussed the more practical issues of attribution. Ms. Lillemets also elaborated that there were political concerning in attributing, even if you are able to successfully attribute:

> *"In the 2007 attack, some politicians said it was Russia but officially did not attribute to Russia. When you do this you can trace it, and then consider whether you want to name the person, because when you do you reveal the extent of your capabilities."*

She went on to state that when a state does reveal the extent of their abilities, they face the possibility of opening themselves up to further targeting. This is another aspect of the reflexive opportunity that is presence in the cyber domain and influences the handling of cyber security.

There was an understanding that because Estonia is a cyber society, this attracts negative attention in the form of cyber attacks and cyber crime, whether state sanctioned or not.

Another aspect to the attribution problem that was very clear was the apparent lack of necessity for it. When this topic came up and interviewees were asked to elaborate, they did not imply that attribution was a main concern when it came to Estonian cyber security:

> *"You don't need to know exactly who is behind the threat, because the threat can come from around the world, you can't possibly identify all the threat sources or threat vectors…what you can do is protect your systems so that whoever is behind the attack or whatever might happen, if you keep in mind these aspects you are more or less are safe."*
> – Raul Rikk, EGA

The sentiment shown by Mr. Rikk's statement exemplifies the understanding that the knowledge of who is attacking you from where does not help in the actual protecting of systems. This is because the Estonian mindset when it comes to cyber security is that you must assume someone is always trying to attack you, so you must instead be ready at all times. Ms. Lillemets also showed this sentiment:

> *"It is harder to know if there is going to be an attack on your systems, but making sure everyone knows their basic cyber security isn't."*

Estonian experts were less concerned with the who and why than with the issue of resilience and preparedness. This is clearly shown in their emphasis on resilience and building an agile system that can withstand a multitude of attacks and problems. This is a response to the nature of the cyber domain, and the lack of clear threat that is presence. Estonian policy-makers had to focus on building a system which was resilient to withstand a number of attack, and in essence be ready for whatever the future might bring, because there was an inability to know what attacks were coming.

Evolution of Policies

Interviewees also made a point to discuss the evolution of the national cyber security strategy of Estonia, saying that strategy has gone from one which was a reaction to the 2007 attack to one which is more forward looking:

> *"In our case it all started in 2007, from point of view of strategy planning it was quite a security matter for us, the cyber attacks…The first one addressed security framework, the next one was focused on upgrade, and enhanced early warning, resilience, awareness, and now were are preparing third one."*
>
> – Uku Särekanno, RIA

> *"I think our first strategy was more reactive, but now the new one is more proactive, we are looking at possibilities if we cannot do it. And what will happen if we fail to meet these goals, basically we are forward looking."*
>
> – Madis Raaper , MEAC

Here we see a progression in the cyber security strategies from being reactive to being proactive. Estonian experts and policy-makers initially acted due to the 2007 attacks, but as the cyber security of Estonian began to be taken more seriously, there was a deeper understanding of the nature of the cyber domain that flourished. The understanding of the cyber domain has pushed Estonian policy-makers to take cyber security strategy down a different road than conventional security strategies have take. This has been the case with the second strategy and this trend will continue with the third strategy, which has yet to be published:

> "*The thing is we are drafting third strategy and what we did different is we included everyone who is someone in cyber, including private sector, IT companies, other government institutions, and university, absolutely, and we had seminar and they gave us their input and they gave us their feedback."*
>
> – Madis Raaper

Mr. Alatalu described the first cyber security strategy as being very concerned with the aftermath of the 2007 attack, but then that the next strategy had been more focused on building skills and resilience in the system. The third strategy, he says, is even more forward looking, looking "beyond the horizon", and focuses on issues such as artificial intelligence and data leaks, as well as focusing on broader question such as how society works through cyber. Estonian policy-makers are striving to improve the already high level of security integration with the next

strategy. Not only are they involving more and more relevant parties, but they are also trying to consider more possible areas to consider in strategy, areas of development that will produce unknown risks.

Conclusions

To conclude this paper, I will summarize my arguments and the outcomes of the empirical case study. I will give an overview of my characterization of the cyber domain along with the theoretical framework with which I explain the understand of cyber security. I will then give a final conclusion for the case of Estonian cyber security discourse, stating the overall findings of my research.

I have argued that the understanding and functioning of security in the domain of cyberspace is fundamentally different to that of conventional military security. The cyber domain is differentiated from traditional domains of security by its borderless nature, the reflexive risk which dictates cyber opportunity, and the proactive nature of its strategies and policies. These characteristics cannot be adequately understood by conventional security theory, but can be explained by Beck's theory on risk society. The borderless features of the cyber domain is characteristic of the blurring of traditional borders which is seen in a risk society. These disappearing borders include defined threats and defined actors, in terms of threat actors and security providers. This is also seen in the lack of physically boundaries in the cyber domain, and the difficulty of setting national borders. Lastly, cyberspace encompasses all sectors of society: public, private, and civilian.

The cyber domain is also governed by the reflexive nature of its innovation and advances. The risks are self-generated, and the more a society continues to advance the more at risk it is. This is one of the defining features of the cyber domain. The main security risks are not from outside actor, but from the modern institutions which society has created. This reflexive nature and the importance of systemic risks is overlooked when considering the cyber domain from a traditional understanding of security, in which threats have very strictly defined actors and objects. However, by looking at the cyber domain from a risk society understanding, we can see that these systemic risks are characteristics of new modernity, which is reflexive due to our continued advancements. Without the creation of cyberspace and e-society, there would be no risk. However, it is the awareness of this reflexive nature which has changed the way the cyber security is understood and dealt with. This awareness has a profound effect on the direction of

cyber security strategy, making strategy proactive rather than reactive. This is because of the nature of the cyber domain, which prevents society from being about to predict what threats we might face. This is why cyber security strategy focuses on resilience and agility, so that it might be prepared for the onslaught of systemic risks and unknown threats that it faces every day. This focus on resilience and agility is an example of the presence of the future as explained by risk society theory. Due to the awareness of the nature of the cyber domain, policy-makers focus cyber security strategy on preparedness because of this ever-present risk.

The understanding of the cyber domain by Estonian policy-makers and stakeholders is consistent with this analysis in several ways. Firstly, cyber security is seen as being borderless. Experts both stated that it is difficult to differentiate what is national cyber security because it quickly becomes global. Likewise, there is a difficulty of pinpointing specific threats. Cyber security stands apart from traditional security because policy makers and stake holders are unable to predict threats and plan accordingly. There is an understanding that there are too many risks in the cyber realm. Rather than focus on specific scenarios, cyber security must focus on planning for system failure and making secure that the critical infrastructure is resilient. We can see and understanding that this is the way policy-makers view risk and the cyber domain through adopting risk society theory as a means of analysis. Estonian cyber security strategy does not attempt to classify and identify all the threat vectors, nor does it monopolize the practicing of cyber security in Estonia, and we can understand why when we look at their actions and words through this specific theoretical lens.

Estonian cyber security experts are aware of the reflexive nature of the risks in cyberspace. Policy makers do not view cyber security as a goal that can be achieved, it is an ongoing process of risk management rather than securing totally. This understanding is seen in the nature of Estonia cyber security policy and strategies, which focus on resilience and agility of Estonian cyberspace. These strategies are proactive in nature rather than reactive, and have a significant presence of the future in that they seek to be ready for unknown risks. This is evident in the large amount of importance that Estonian policy makers place on cyber awareness and education, and through their concept of cyber hygiene. This aids in the ongoing process of cyber resilience by attempting to manage the risks that are created by everyday users.

The understanding of cyber security by Estonian policy makers and stake holders coincides with that of a risk society, and we can understand their departure from conventional approach and treatment of security to a more risk-based and resilience-based approach. Experts characterize the cyber domain as borderless, and differentiate cyber security from 'conventional security', and this has a significant impact on the nature of strategies and policies. Perhaps most importantly, Estonian experts are aware of the reflexive nature of cyber opportunity and the systemic risk which dictates the domain. This awareness is what makes a risk society a risk society, and what guides Estonian cyber security strategy and policy down a proactive path rather then a reactive path. By looking at the cyber domain and the treatment of cyber security through this lens, we can understand why policy-makers and stakeholder conceptualized cyber risk and security in the way that they do.

REFERENCES

References

Areng, Liina. Lilliputian States in Digital Affairs and Cyber Security. CCDCOE, 11 June 2015, ccdcoe.org/multimedia/lilliputian-states-digital-affairs-and-cyber-security.html.

Bajerova, Alzbèta. "Impact on NATO of Cyberspace as a Domain of Operations." 2017. NATO CCD COE Publishing.

Beck, U. (2001) World Risk Society (London: Blackwell).

Beck, U. (1995) Risk Society; Ecological Politics in an Age of Risk (Cambridge: Polity).

Beck, U. (1994) 'The Reinvention of Politics', in Reflexive Modernisation: Politics, Tradition and Aesthetics in the Modern Social Order (Stanford: Stanford University Press).

Beck, U. (1992) Risk Society: Towards a New Modernity (London: Sage).

Beck, Ulrich, et al. "The Theory of Reflexive Modernization*." Theory, Culture & Society*, vol. 20, no. 2, 2003, pp. 1–33., doi:10.1177/0263276403020002001.

Brangetto, Pascal, and Mari Kert-Saint Aubyn. "Economic Aspects of National Cyber Security Strategies." CCDCOE, 10 June 2016

Cavelty, Myriam Dunn. "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse." *International Studies Review*, Wiley/Blackwell (10.1111), 10 Apr. 2013,

Czosseck, Christian, et al. “Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security.” *International Journal of Cyber Warfare and Terrorism* (IJCWT), IGI Global, 1 Jan. 2011

Deibert, Ronald & Rohozinski, Rafal. (2010). ‘Risking Security: Policies and Paradoxes of Cyberspace Security’. *International Political Sociology*. 4. 15 - 32.

Elbe, S. (2008) ‘Risking Lives: AIDS, Security and Three Concepts of Risk’, *Security Dialogue* 39(2–3): 177– 198.

Estonian National Cyber Security Strategy 2014 – 2018. Available at: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

‘E-stonia Facts’. Available at: https://e-estonia.com/wp-content/uploads/updated-facts-estonia.pdf

Geers, Kenneth (2009) ‘The Cyber Threat to National Critical Infrastructures: Beyond Theory’, *Information Security Journal: A Global Perspective*, 18:1, 1-7, DOI: 10.1080/19393550802676097

Hansen, Lene, and Helen Nissenbaum. “Digital Disaster, Cyber Security, and the Copenhagen School.” *International Studies Quarterly,* vol. 53, no. 4, 2009, pp. 1155–1175., doi:10.1111/j.1468-2478.2009.00572.x.

Harknett, Richard & A. Stever, James. (2009). ‘The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen’. *Journal of Homeland Security and Emergency Management*.

Heng, Y.-K. (2006) ‘The “Transformation of War” Debate: Through the Looking Glass of Ulrich Beck’s World Risk Society’, *International Relations,* vol. 20, no. 1 , pp. 69-91.

ISO/IEC. ISO/IEC 27002: code of practice for information security management 2005.
Deibert, R. J. and Rohozinski, R. (2010), Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, 4: 15-32.

Krahmann, E. (2010) 'Beck and Beyond: Selling Security in the World Risk Society', *Review of International Studies* 36(3): 1-20.

Nyman Metcalf, Katrin. "A Legal View on Outer Space and Cyberspace: Similarities and Differences." CCDCOE, 21 Feb. 2018

Nissenbaum, Helen. "Where Computer Security Meets National Security." Ethics and Information Technology, Kluwer Academic Publishers, 2005.

Ottis, Rain, et al. Cyber Society and Cooperative Cyber Defence. CCDCOE, 16 June 2015.

Osula, Anna-Maria, and Kadri Kaska. "National Cyber Security Strategy Guidelines." 2013. NATO CCD COE Publishing.

O'Connell, Mary E. "Cyber Security without Cyber War." *Journal of Conflict and Security Law*, vol. 17, no. 2, 2012, pp. 187–209., doi:10.1093/jcsl/krs017.

Rasmussen, M.V. (2001) 'Reflexive Security: NATO and International Risk Society', Millennium 30(2): 285- 309.

Rasmussen, M.V. (2004) '"It Sounds Like a Riddle": Security Studies, the War on Terror and Risk', *Millennium* 33(2): 381-395.

Schmitt, Michael N., and Liis Vihul. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017.

Schmitt, Michael, and Liis Vihul. The Nature of International Law Cyber Norms. CCDCOE, 31 Dec. 2014.

Tikk, Eneken. “Ten Rules for Cyber Security.” Survival, vol. 53, no. 3, 2011, pp. 119–132., doi:10.1080/00396338.2011.571016.

Von Solms, Rossouw, and Johan van Niekerk. “From Information Security to Cyber Security.” Computers & Security, Elsevier Advanced Technology, 29 Apr. 2013

Williams, M.J. (2008) ‘(In)Security Studies, Reflexive Modernization and the Risk Society’, *Cooperation and Conflict* 43(1): 57–79.

I, _____

(*author's name*)

(personal code _____),

herewith grant the University of Tartu a free permit (non-exclusive licence) to:

_____
_____
_____,

(*title of thesis*)

supervised by _____,

(*supervisor's name)*

1. To reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright.
2. To make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright.
3. I am aware that the rights stated in point 1 also remain with the author.
4. I confirm that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, _____ (*date*)

_____ (*signature*)